

The Passive Eavesdropper Affects my Channel: Secret-Key Rates under Real-World Conditions — Extended Version —

Christian Zenger, Hendrik Vogt, Jan Zimmer, Aydin Sezgin, Christof Paar
Ruhr-Universität Bochum, Germany

{christian.zenger, hendrik.vogt, jan.zimmer, aydin.sezgin, christof.paar}@rub.de

Abstract—Channel-reciprocity based key generation (CRKG) has gained significant importance as it has recently been proposed as a potential lightweight security solution for IoT devices. However, the impact of the attacker’s position in close range has only rarely been evaluated in practice, posing an open research problem about the security of real-world realizations. Furthermore, this would further bridge the gap between theoretical channel models and their practice-oriented realizations. For security metrics, we utilize cross-correlation, mutual information, and a lower bound on secret-key capacity. We design a practical setup of three parties such that the channel statistics, although based on joint randomness, are always *reproducible*. We run experiments to obtain channel states and evaluate the aforementioned metrics for the impact of an attacker depending on his position. It turns out the attacker himself affects the outcome, which has not been adequately regarded yet in standard channel models.

I. INTRODUCTION

The inherent randomness of the wireless medium can be utilized for extracting a shared secret, since wireless channels exhibit the feature of *reciprocity*. This approach is referred to as channel-reciprocity based key generation (CRKG). The underlying assumption is that an eavesdropper (Eve) cannot obtain the same channel state, and thus cannot compute the key. The general feasibility of the approach has been reported by several early works in the literature [1], [2], which have been extended by subsequent studies related to practical key agreement [3], [4]. In particular, there have been some works that deal with the removal of temporal correlation, by methods like principal component analysis (PCA) [5], beamforming [6] or linear prediction [7].

Throughout the paper, we use *cross-correlation*, *mutual information*, and *secret-key rates* as performance metric. The theoretical foundation of secret-key rates has been established by Maurer [8] and Ahlswede et al. [9]. They coined the information-theoretic *source-type model*, where Alice, Bob and Eve have access to a jointly random source, and derived bounds on the secret-key *capacity*. Their result is used in a large body of research, especially for Gaussian channels, e.g., reference [10] for a multi-observation model or [2] for the application to UWB channels.

However, some of the popular beliefs regarding the capabilities of the eavesdropper have to be challenged. Many previous works, e.g., [11], [12], have relied on the assumption

that the channel of Alice-to-Bob gets uncorrelated to that of Eve, as long as Eve is positioned more than half a wavelength away from Alice and Bob, commonly referred to as Jake’s model [13, Chapter 3.2.1]. In the literature, this is usually referred to as *spatial decorrelation* [14]. A study [4] has questioned this assumption by practical evaluation. Recently, a comprehensive study [15] has shown that for many popular correlation models of scattering environments, the eavesdropper might obtain largely correlated observations, especially if Eve is located within the line-of-sight beam of Alice and Bob.

In this work, we intend and shed more light on the threats for CRKG from passive eavesdropping. As a consequence, we extend the work of [15] by providing more elaborated practical measurements. We quantify the leakage of Alice and Bob in relation to Eve with respect to the distance, especially for low ranges that introduce near-field effects. The measurement setup is designed with the objective to generate *reproducible* results, such that we can justify *stationary* random processes. This is a fundamental necessity in order to obtain meaningful results, which has sometimes been overlooked in previous work. The cross-correlation and achievable secret-key rate serve as the performance metrics that indicate the common randomness available to Alice and Bob, and likewise, the information loss to Eve. We evaluate the metrics for the original data and the processed versions after down-sampling or decorrelation. The results demonstrate that the close physical presence of Eve in the communication setting significantly changes the channel statistics. This phenomenon is so far not covered by conventional channel models for CRKG.

Section II introduces the system model and elaborates on both the processing of the measured data and the performance metrics on security. The measurement setup is described in section III. The evaluation and results of the measurement campaign are presented in section IV. Finally, section V concludes the paper.

II. SYSTEM MODEL

As depicted in Figure 1, we consider Alice, Bob and Eve measuring the channel $h_{ab,k} \in \mathbb{R}$, $h_{ba,k} \in \mathbb{R}$, $h_{ae,k} \in \mathbb{R}$ and $h_{be,k} \in \mathbb{R}$, which represent the state of Alice-to-Bob, Bob-to-Alice, Alice-to-Eve and Bob-to-Eve channels, respectively, and k denotes a discrete time instant. We model these variables

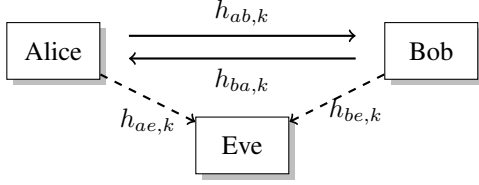


Fig. 1. Overview of the system model.

as joint stationary and ergodic random processes. In general, Eve gets two channel states $(h_{ae,k}, h_{be,k})$, however, in this study we focus on $h_{ae,k}$ only. In the following, we use the labels $x_k := h_{ba,k}$ for Alice, $y_k := h_{ab,k}$ for Bob, and $z_k := h_{ae,k}$ for Eve. Furthermore, we define the vector process $\mathbf{v}_k := (x_k, y_k, z_k)^T$.

A. Processing

For different k , the random vectors \mathbf{v}_k are likely to exhibit correlation in time, since the wireless channel is varying only slowly in indoor environments. In order to remove the temporal dependencies, we perform two alternative options of processing, namely either downsampling or decorrelation. We show both options for x_k only, since we have the same processing for y_k and z_k .

1) Downsampling

If we keep only every N_m th variable of the process x_k , we effectively downsample by factor N_m and obtain

$$x_k^{\text{ds}} = x_{kN_m}. \quad (1)$$

The generated x_k^{ds} can be assumed independent under the condition that the process does not exhibit any dependence after an interval of N_m variables. Subsequently, we assume that the $\mathbf{v}_k^{\text{ds}} = (x_k^{\text{ds}}, y_k^{\text{ds}}, z_k^{\text{ds}})^T$ are identically and independently distributed (i.i.d.) for different k .

2) Decorrelation

We need to provide an estimator for the autocorrelation function

$$\hat{r}_{xx}[l] = \frac{1}{N-l} \sum_{i=0}^{N-l-1} x_i x_{i+l}. \quad (2)$$

This estimator is unbiased if the process is correlation-ergodic. The linear forward predictor for x_k of order N_m is given by

$$\hat{x}_k = \sum_{i=1}^{N_m} a_i x_{k-i}, \quad (3)$$

where $a_i \in \mathbb{R}$ are parameter coefficients, which can be computed by Levinson-Durbin recursion based on Yule-Walker equations [16]. We define

$$x_k^{\text{de}} = x_k - \hat{x}_k \quad (4)$$

as *innovation sequence*, which is orthogonal to past $h_{ab,k-i}$ for $i > 0$. However, orthogonal (or uncorrelated if zero-mean) variables do not necessarily imply independence, especially not *joint* independence of $\mathbf{v}_k^{\text{de}} = (x_k^{\text{de}}, y_k^{\text{de}}, z_k^{\text{de}})^T$ for different

k . Decorrelation is practically more relevant than downsampling (even if no i.i.d. can be achieved), since the information loss is significantly lower.

B. Performance metrics

Throughout the paper, we use (1) the Pearson correlation and (2) secret-key rates as performance metrics for security.

1) Pearson correlation

The Pearson correlation provides a measure of linear dependence between two data series. The values span between -1 and 1 , where 1 refers to absolute correlation, 0 to no correlation, and -1 to perfect inverse correlation. It is a wide-used metric for secrecy of practical secret-key generation [15]. Given a finite collection of N pairs (x_k, y_k) from the process, we use the estimator

$$\rho_{xy} = \frac{\sum_{i=0}^{N-1} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=0}^{N-1} (x_i - \bar{x})^2} \sqrt{\sum_{i=0}^{N-1} (y_i - \bar{y})^2}}, \quad (5)$$

where $\bar{x} = \frac{1}{N} \sum_{j=0}^{N-1} x_j$ and $\bar{y} = \frac{1}{N} \sum_{j=0}^{N-1} y_j$ are the sample means.

2) Secret-key rate

We introduce the information-theoretic secret-key rate and use the downsampled process (1). Recall that the \mathbf{v}_k^{ds} are i.i.d. We characterize \mathbf{v}_k^{ds} by the joint probability density function $f_{\mathbf{v}_k^{\text{ds}}}$. We apply a lower bound on secret-key capacity based on the source-type model, under the following conditions:

- 1) The joint probability density function $f_{\mathbf{v}_k^{\text{ds}}}$ is known a priori at all terminals.
- 2) Alice and Bob exchange messages over an authenticated, public channel with unlimited communication capacity.
- 3) Eve remains passive at all times.

Subsequently, the asymptotic bound is given by [9]

$$C_{\text{sk}} \geq \mathbb{I}(x_k^{\text{ds}}; y_k^{\text{ds}}) - \min [\mathbb{I}(x_k^{\text{ds}}; z_k^{\text{ds}}), \mathbb{I}(y_k^{\text{ds}}; z_k^{\text{ds}})] =: R_{\text{sk}} \quad (6)$$

for each k , since the process is stationary. Since the actual probability distributions are unknown in practice, we evaluate the lower bound (6) by estimations, based on a finite number of measured samples. We utilize a k -nearest neighbor estimator (NNE) for the mutual information, which is based on the idea and implementation of [17]. Mutual information is a function of joint and marginal probability densities. For a measure of the joint density, the estimator computes the distance between a tuple of samples and its k th-next neighbor. A similar approach is provided for the marginal densities. To best of our knowledge, the reliability of the NNE has not been studied systematically. However, results in [17] indicate that at least for multivariate Gaussian variables, the estimation error is very low if $N > 10^4$ samples are used for the estimation.

Note that the bound (6) could have been defined with the original \mathbf{v}_k or the decorrelated processes (4), such that less information is discarded than in case of downsampling.

However, in order to obtain an accurate estimation of (6), we require i.i.d. samples for the two following reasons:

- 1) The bound (6) has been derived under the assumption of an unlimited number of i.i.d. observations from a random source. Therefore, a value of R_{sk} measured in bits per observation, is meaningful only if the time series is i.i.d. as well.
- 2) The NNE of [17] requires i.i.d. samples, since it relies on Khinchin's theorem [18, p. 277]. If the time series of samples exhibits some dependence in time, the estimator might induce an undesired bias.

Therefore, if we apply the process v_k or its decorrelated modification (4), we have an approximation of the lower bound R_{sk} (6) only. While approximating the common information of Alice and Bob is a rather "safe" option, we need to be cautious regarding Eve. In order to minimize the risk of underestimating Eve, we verify our results obtained from v_k or the decorrelated version (4) by comparing them with the downsampling approach, since it provides a more accurate description of the information leakage to Eve. Unfortunately, by removing samples from the estimation, the NNE gets more biased.

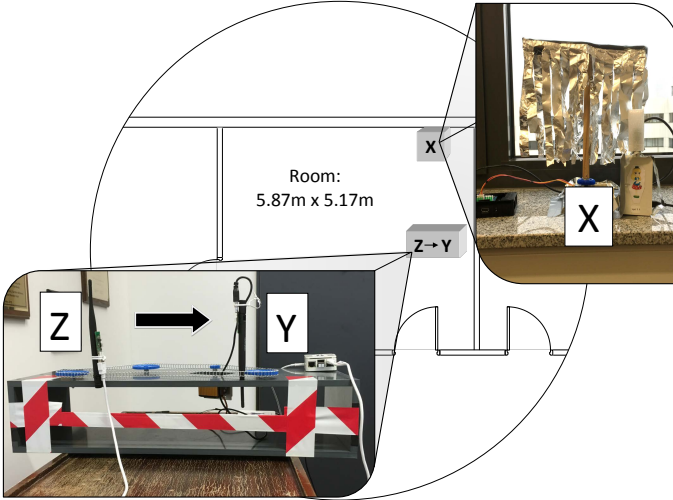


Fig. 2. The testbed includes several experimental setups for performance evaluation as well as for security analysis. Alice (X), Bob (Y) and Eve (Z) are mounted on a automated antenna positioning system.

III. MEASUREMENTS

The testbed is applied at the premises of our research group, which is an office area in a university building. Alice is positioned at a predestined access point position. Bob and Eve are mounted on an automated antenna positioning setup, which is located at several predestined "end-device" positions (cf. Figure 2). For this, we choose positions which are representative for security-related IoT devices, such as doorknobs (keyless entry systems), window frames (perimeter fence intrusion sensor), and wall (motion detectors) positions. Due to a lack of space, in this version of the paper we restrict ourselves to a description of one representative realization of

TABLE I
PARAMETERS OF THE MEASUREMENT SETUP

Parameter	Variable	Value
Sampling interval	T_s	100 msec
Probing duration	T_p	< 5 msec
Step size	Δ_d	5 mm
Accuracy of step size	$\hat{\Delta}_d$	± 0.05 mm
Geometrical distance Bob-Eve	Δ_{BE}	[0, 30] cm
Geometrical distance Alice-Bob	Δ_{AB}	5 m
Samples per step	N	$3 \cdot 10^5$

all experiments. We will also provide a full version of the paper with results of 23 further positionings in the building.

We perform mobile, long-time narrow-band channel measurements on 2.4 GHz (wavelength 12.5 cm). The data exchange protocol is implemented on three Raspberry Pi 2 platforms (credit-card sized computer). All devices are equipped with a CC2531 USB enabled IEEE 802.15.4 communication interface¹. The CC2531 is a true SoC solution for IEEE 802.15.4 applications, that is compatible to network layer standards for resource-constrained devices: ZigBee, WirelessHART, and 6LoWPAN. The platform is equipped with proprietary PCB antennas, i.e., *Meandered Inverted-F antenna* (MIFA), with the size of 5×12 mm. These antennas provide good performance with a small form factor. The platform and antenna design are widely used in commercial products and suited for systems where ultra-low-power consumption is required.

In order to establish common channel probing, Alice periodically sends data frames to Bob and waits for acknowledgments. Eve also receives these request-response pairs. When receiving a probe, all three devices extract Received Signal Strength Indicators (RSSI) values and, thus, can measure a channel-dependent sequence over time. For evaluation of the channel measurements, we store and process the realizations of $v_k := (x_k, y_k, z_k)^T$, locally on a monitoring laptop.

Table I lists the relevant parameters of our measurement setup. We obtain a complete realization of v_k on every sampling interval $T_s = 100$ msec. The protocol ensures that Alice, Bob, and Eve can probe the channel within a probing duration $T_p < 5$ msec. We want to analyze the joint statistical properties of the samples with respect to the position of Eve in the scene. As a consequence, we apply an automated antenna positioning system, which is constructed from a low-reflective material, cf. Figure 2. It moves the antenna of Eve on a linear guide towards the fixed antenna of Bob in step size $\Delta_d = 5$ mm with accuracy $\hat{\Delta}_d = \pm 0.05$ mm. The variable distance Δ_{BE} ranges from 0 to 30 cm in order to provide 60 different locations. Alice's antenna is placed orthogonal to the linear guiding at a fixed distance $\Delta_{AB} = 5$ m. For each position of Eve's antenna, we record at least N samples.

Alice and Bob extract the common randomness x_k and y_k from a time-varying channel. Since we aim for meaningful and

¹<http://www.ti.com/tool/cc2531emk>

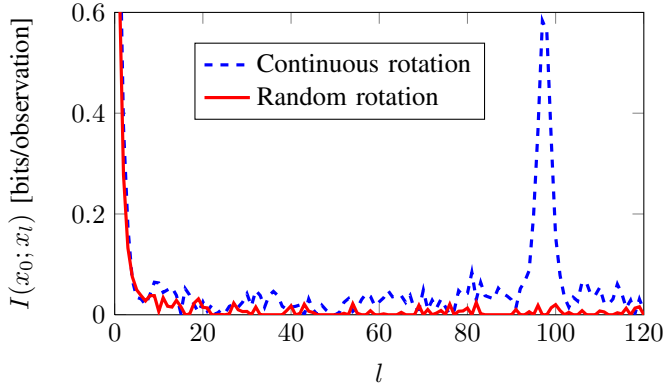


Fig. 3. Self-dependence of channel gains with respect to time delay. Setup is equipped with aluminum strips of either continuous or random rotation.

reproducible results, we have to create an environment which provides the joint stationarity to the random process. Therefore, with a distance of 10 cm to Alice’s antenna, we deploy a curtain of 30×30 cm aluminum strips that continuously rotates at ≈ 0.1 rotations per second, cf. Figure 2. However, the rotation itself inserts a deterministic component into the channel. The evolution of the self-dependence of channel gains — we show exemplary x_k^{ds} — is illustrated in Figure 3. It shows that the mutual information decays rapidly and vanishes after four samples, corresponding to approximately 400 ms. However, due to the continuously rotating curtain of aluminum strips, we discover strong stochastic dependencies after 96 samples, corresponding to approximately 9.6 s. Therefore, we adapt a random source (Unix file `/dev/urandom`) to the motor controller and program the instrument to rotate with random speed between 0.240 rad/s and 1 rad/s in random direction and with random interval lengths $0^\circ, 1^\circ, \dots, 60^\circ$ (uniformly distributed). Figure 3 shows that no strong stochastic dependencies are given anymore.

IV. EVALUATION AND RESULTS

We now use the experimental measurements to evaluate and compare the results of the Pearson correlation (5), mutual information, as well as the achievable bound of the secret-key capacity (6), as a function of attacker’s distance Δ_{BE} to Bob. We interpret the original measurements as realizations of v_k . In addition, we have the decorrelated and downsampled outcomes, denoted by the processes v_k^{de} and v_k^{ds} , respectively. The decorrelated samples are obtained by a linear prediction of order $N_m = 30$. To generate the i.i.d. random vectors v_k^{ds} we downsample v_k by the factor $N_m = 30$. In subsection II-B2, we have already outlined the necessity of i.i.d. random vectors to obtain accurate estimations. This is not given for v_k and v_k^{de} , however, they provide valid approximations, as the results indicate later on. We present three Figures 4, 5, 6 with three Subfigures a)-c) each, which are arranged in a 3x3 matrix on the next page. The *rows* denote the Figures as follows.

- 1) Fig. 4 illustrates the results for the *original* process v_k .

- 2) Fig. 5 shows the results for the *downsampled* process v_k^{ds} of (1).
- 3) Fig. 6 depicts the results for the *decorrelated* process v_k^{de} of (4).

The *columns* constitute Subfigures as follows. For convenience, we introduce generic labels $X \in \{x_k, x_k^{\text{de}}, x_k^{\text{ds}}\}$ for Alice, $Y \in \{y_k, y_k^{\text{de}}, y_k^{\text{ds}}\}$ for Bob and $Z \in \{z_k, z_k^{\text{de}}, z_k^{\text{ds}}\}$ for Eve.

- 1) Subfigures a) show the Pearson correlation (5) vs. geometrical distance Δ_{BE} between the three pairs (Alice \leftrightarrow Bob ρ_{XZ} , Alice \leftrightarrow Eve ρ_{XY} , Bob \leftrightarrow Eve ρ_{YZ}).
- 2) Subfigures b) zoom into the correlation ρ_{XY} of Alice \leftrightarrow Bob.
- 3) Subfigures c) depict the three mutual information results ($I(X; Y)$, $I(X; Z)$, $I(Y; Z)$) and the secret-key rate R_{sk} of (6) vs. geometrical distance Δ_{BE} .

Most of the practical key generation schemes use downsampling or decorrelation on the original observations v_k . We introduce the Figs. 4, 5 and 6 in order to analyze whether downsampling and decorrelation obscure certain features of the channel that are important for the security evaluation of the system. We start with a comparison of the cross-correlation behavior between Alice and Bob, as well as to a potential attacker. By comparing Figure 4 (a-b) and Figure 5 (a-b) we see that no significant differences in ρ_{XY} and ρ_{XZ} occur after downsampling. (Further, ρ_{XZ} and ρ_{YZ} are almost identical due to channel reciprocity between Alice and Bob.) The high similarity is due to the fact that even the process v_k does not exhibit much dependency in time, as already hinted in Figure 3. As a consequence, the results obtained for v_k expose a valid approximation of the cross-correlation. As it can be seen from Figure 5, in case of downsampling the results are more noisy, since much fewer samples are available for the estimations.

After decorrelation, the results (see Figure 6) show that (unlike in case of downsampling) the correlation decreases on average by ≈ 0.05 , which can have a significant negative impact on the performance of a potential quantization scheme, cf. [19, Figure 3]. Furthermore, the difference between the minimum and maximum value significantly decreases. Whereas in the original (and downsampled) signal the difference is $0.995 - 0.98 = 0.015$, the difference is $0.97 - 0.89 = 0.08$ for the decorrelated signal. This probably stems from errors of the autocorrelation estimate (2), which is necessary for the linear forward prediction. Another reason might be the Pearson correlation where single outliers (e.g., strong peaks) significantly influence the result. Analyzing the impact of decorrelation techniques on the reciprocity and security in detail is left for future work.

By analyzing the attacker’s opportunity, we observe a wavelength dependent behavior of the correlation between z_k and x_k (or y_k), as illustrated in Subfigures a). The following findings hold for all three processes: $v_k, v_k^{\text{ds}}, v_k^{\text{de}}$. The correlation vs. distance function ρ_{XZ} (and ρ_{YZ}) looks similar to the channel diversity function known from Jake’s model [13],

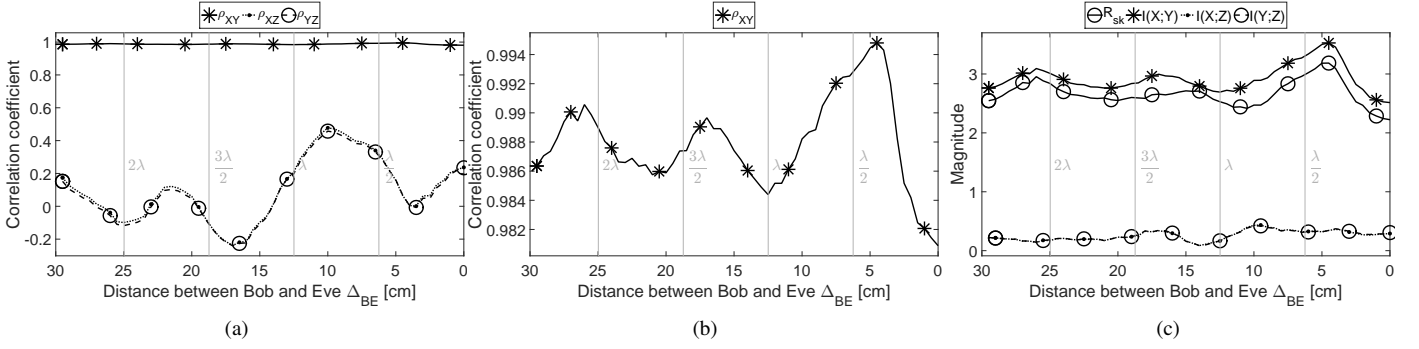


Fig. 4. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given.

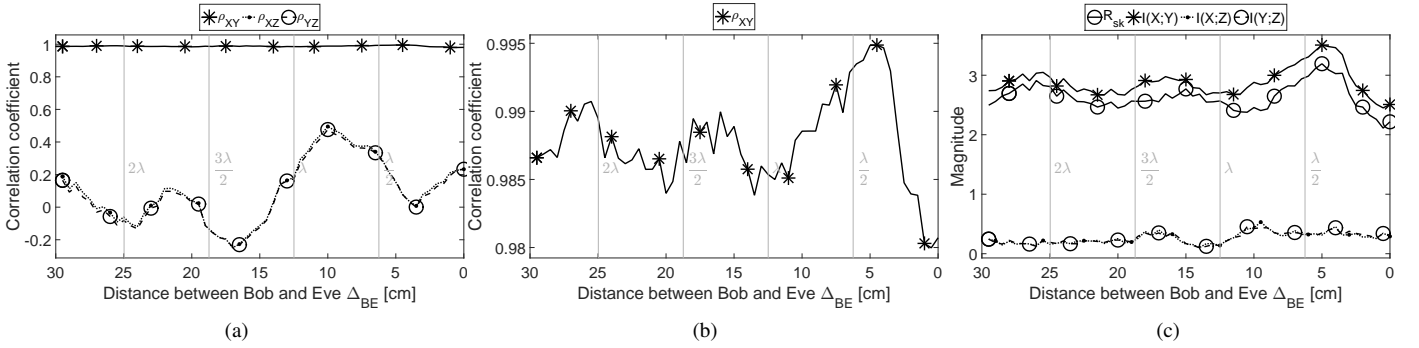


Fig. 5. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given.

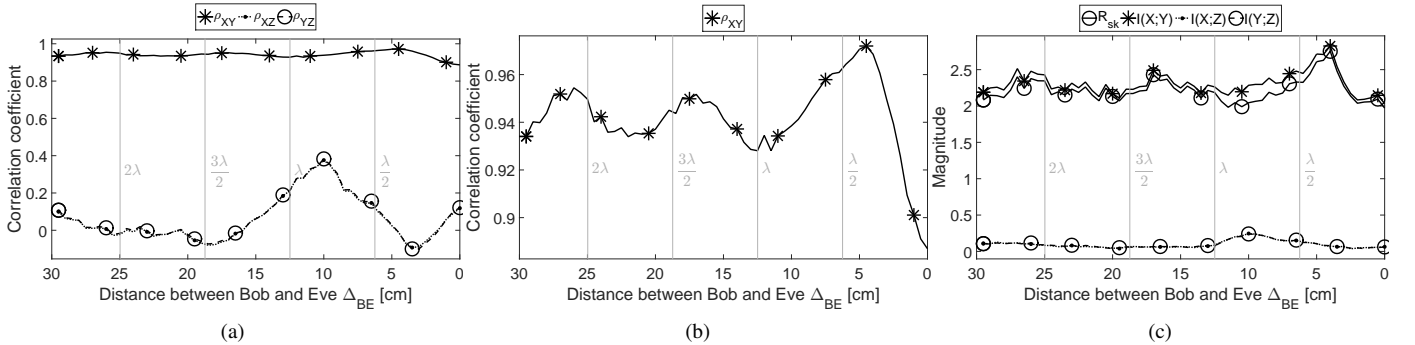


Fig. 6. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given.

which is a zero-order Bessel function² (cf. Figure 7). However, the highest correlation is not at distance $\Delta_{BE} = 0$, where the correlation is only 0.2. The highest cross-correlation is given at a distance of $\Delta_{BE} \approx 12.5$ cm, which is the wavelength of the 2.4 GHz carrier. The first correlation of zero is given at a distance of 4 cm.

Note that the cross-correlation behavior of x_k to y_k is not independent of Eve's antenna position. Figure 4(b) illustrates the correlation behavior in detail. The correlation has an "oscillating" behavior with a wavelength of approximately

²A zero-order Bessel function is expected for the cross-correlation behavior of two receivers if uniformly distributed scatterers are given. According to Jake's model the first zero correlation is given after $\approx 0.4\lambda$, where λ is the wavelength of the carrier [13], [20].

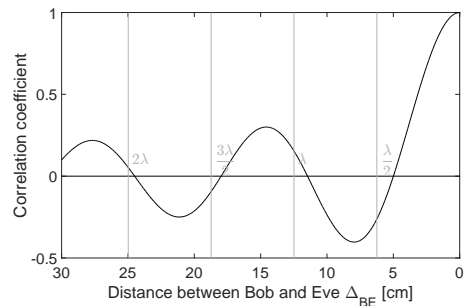


Fig. 7. Bessel function versus distance.

TABLE II
AVERAGED RESULTS OF OUR EXPERIMENT.

	v_k	v_k^{ds}	v_k^{de}
ρ_{x_k, y_k}	≈ 0.99	≈ 0.99	0.94
ρ_{y_k, z_k}	≈ 0.09	≈ 0.09	≈ 0.07
$I(X; Y)$	≈ 2.92	≈ 2.89	≈ 2.31
$I(Y; Z)$	≈ 0.26	≈ 0.27	0.10
R_{sk}	≈ 2.67	≈ 2.63	≈ 2.22

11 cm, whereby at a distance of 5 cm the curve decreases rapidly to the lowest level of ≈ 0.98 . The reason for that might be the non-perfect uniformly distributed scatterers in the environment, which are the basis of Jake's model. The oscillating behavior in Alice's and Bob's original observation is also given in the downsampled and decorrelated versions, cf. Figure 5(b) and Figure 6(b). This behavior is contradictory to theoretical approaches based on Jake's Doppler spectrum [20]. The reason might be because the narrow band fading models do not include coupling and near field effects between both antennas for the spatial evaluation of autocorrelation, cross-correlation, and power spectral density (cf. [13, Chapter 3.2]).

The boundary B between the near field zone and the far field zone can usually be determined by the following relationship: $B \geq \frac{2D^2}{\lambda}$, where D is the largest antenna size [21]. We estimated the size of our antenna to be 6 cm. Therefore, the boundary is ≈ 5.7 cm. Analyzing near field boundaries in detail is left for future work.

Compared to the cross-correlation behavior between the i.i.d. samples x_k^{ds} and y_k^{ds} (after downsampling), both mutual information $I(X; Y)$ and R_{sk} have very similar oscillating behavior, shown in Subfigures c). The (minimum, maximum) values of the correlation are (0.980, 0.995) and the ones of the mutual information are (2.1, 2.75). By analyzing Eve's observation, we see only a slight similarity between the mutual information $I(X; Z)$ (and $I(Y; Z)$) to the correlation behavior of her observation ρ_{XZ} (and ρ_{YZ}). The similarity can be found by comparing the maximum absolute values. For instance, the highest correlation occurs at 10 cm with a value of 0.5, and corresponds to the highest mutual information of 0.5 bits per sample. However, the Bessel-like behavior is not evident. Notably is the fact that the attackers observation z_k does not significantly impact R_{sk} . Our results show that R_{sk} is mainly dependent on x_k and y_k . However, Eve's antenna affects Alice's and Bob's observation and, therefore, affects R_{sk} . Table II summarizes our results.

V. CONCLUSION

In this work, we have provided an important pillar to bridge the gap between theory and practice-oriented approaches for CRKG. Our experimental study helps to provide a better understanding of channel statistics in wireless environments for security applications. We present reproducible results based on a relevant environment which justifies the joint stationarity of a random process. We show results of cross-correlation,

mutual information and secret-key rates, which are dependent on attacker's (or third device's) position. As a result, we discovered that the *observer effect* occurs, which most probably originates from near field distortions. We believe the effect needs to be considered in the future. Common channel models like Jake's model for channel diversity need to be extended in order to be valid for key generation setups. Furthermore, it might be pertinent, for instance, to detect the proximity of Eve. Basing on our results two bidirectionally communicating nodes might recognize a third device, its relative position, and its motion in the proximity. Further studies might use complex-valued channel profiles to analyze third party positioning based and motion based influences.

REFERENCES

- [1] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM workshop on Wireless security*, Los Angeles, CA, USA, Sept. 2006, pp. 33–42.
- [2] R. Wilson, D. Tse, and R. Scholtz, "Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, 2007.
- [3] Y. Liu, S. Draper, and A. Sayeed, "Exploiting Channel Diversity in Secret Key Generation From Multipath Fading Randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, Oct 2012.
- [4] A. Pierrot, R. Chou, and M. Bloch, "Practical limitations of secret-key generation in narrowband wireless environments," *arXiv preprint arXiv:1312.3304*, 2014.
- [5] C. Chen and M. Jensen, "Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, 2011.
- [6] M. Madiseh, S. Neville, and M. McGuire, "Applying Beamforming to Address Temporal Correlation in Wireless Channel Characterization-Based Secret Key Generation," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1278–1287, 2012.
- [7] M. McGuire and A. Movahedian, "Bounds on secret key rates in fading channels under practical channel estimation schemes," in *IEEE International Conference on Communications*, Sydney, AUS, June 2014, pp. 737–742.
- [8] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
- [9] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
- [10] J. Wallace, C. Chen, and M. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *3rd European Conference on Antennas and Propagation (EuCAP)*, March 2009, pp. 1499–1503.
- [11] Suhas Mathur et al., "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *MOBICOM 2008*, 2008, pp. 128–139, formerly known as: mathur2008radio.
- [12] Suman Jana et al., "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *MOBICOM 2009*, 2009, pp. 321–332.
- [13] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.
- [14] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key Generation From Wireless Channels: A Review," *IEEE Access*, vol. 4, pp. 614–626, 2016.
- [15] X. He, H. Dai, W. Shen, P. Ning, and R. Dutta, "Toward proper guard zones for link signature," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2104–2117, March 2016.
- [16] P. Vaidyanathan, *The Theory of Linear Prediction*. Morgan & Claypool, 2007. [Online]. Available: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6813346>
- [17] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Physical Review E*, vol. 69, no. 6, p. 066138, 2004.
- [18] A. Papoulis and S. Pillai, *Probability, Random Variables, and Stochastic Processes*, ser. McGraw-Hill series in electrical engineering: Communications and signal processing. Tata McGraw-Hill, 2002.

- [19] C. Zenger, J. Zimmer, and C. Paar, “Security analysis of quantization schemes for channel-based key extraction,” in *WiComSec-Phy 2015, Workshop on Wireless Communication Security at the Physical Layer, July 22, 2015, Coimbra, Portugal*, 2015.
- [20] E. Biglieri, A. R. Calderbank, A. G. Constantinides, A. Goldsmith, and A. Paulraj, *MIMO Wireless Communications*. Cambridge University Press, 2010.
- [21] T. Dlugosz and H. Trzaska, “How to measure in the near field and in the far field,” *Communications and Network*, vol. 2, no. 1, pp. 65–68, 2010. [Online]. Available: <http://dx.doi.org/10.4236/cn.2010.21010>

APPENDIX A

FULL MEASUREMENT

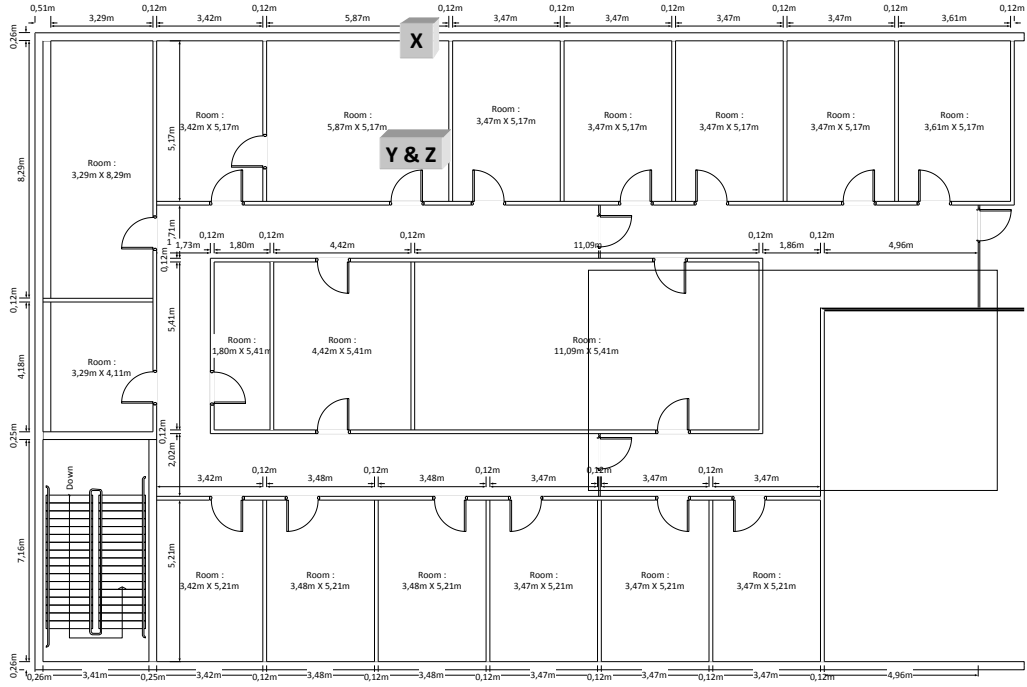


Fig. 8. The testbed includes several experimental setups for performance evaluation as well as for security analysis. Alice (X), Bob (Y) and Eve (Z) are mounted on a automated antenna positioning system.

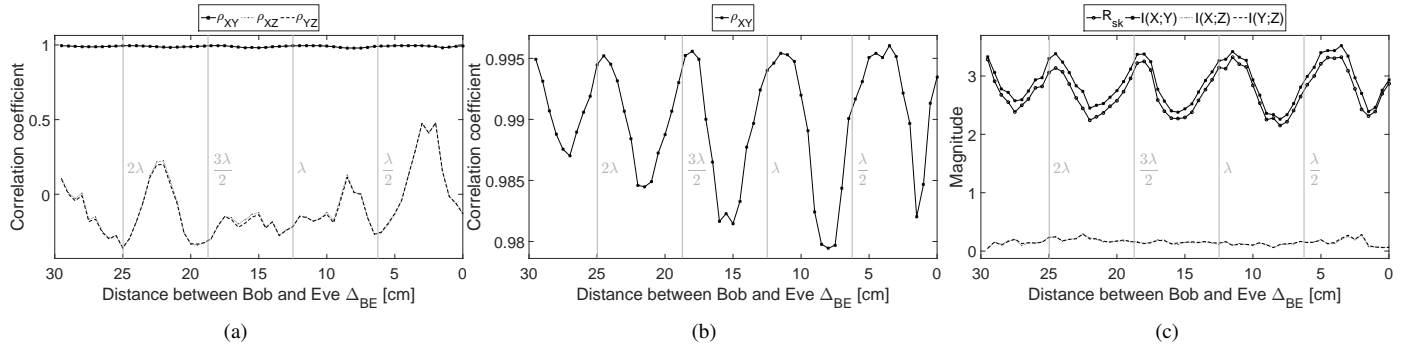


Fig. 9. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 0.

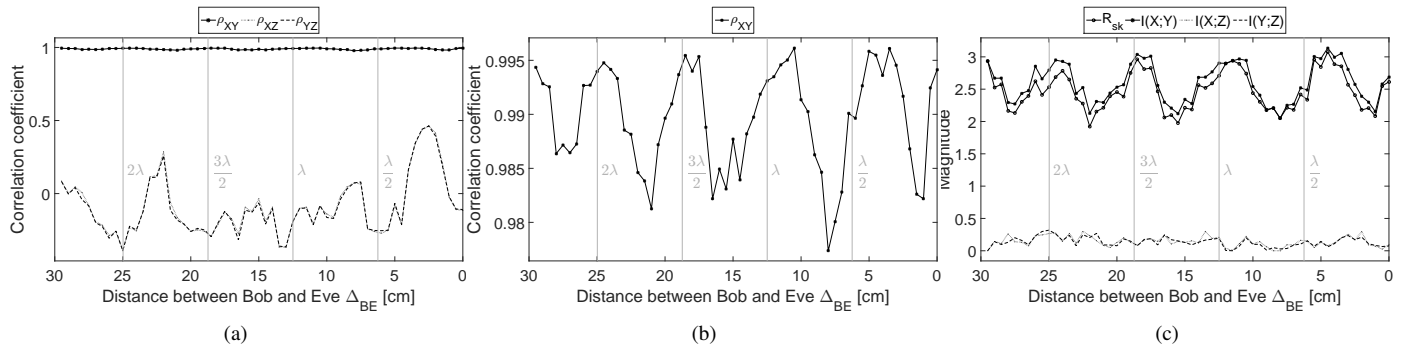


Fig. 10. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 0.

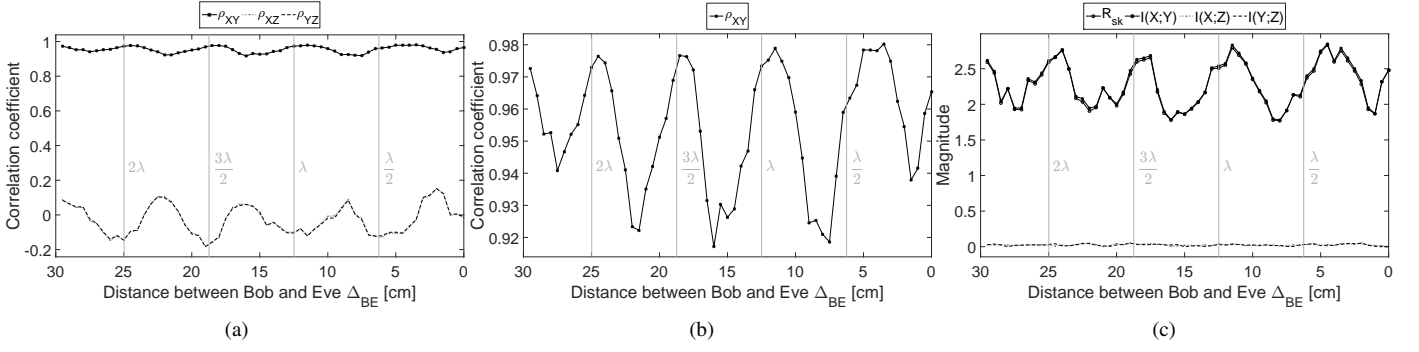


Fig. 11. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 0.

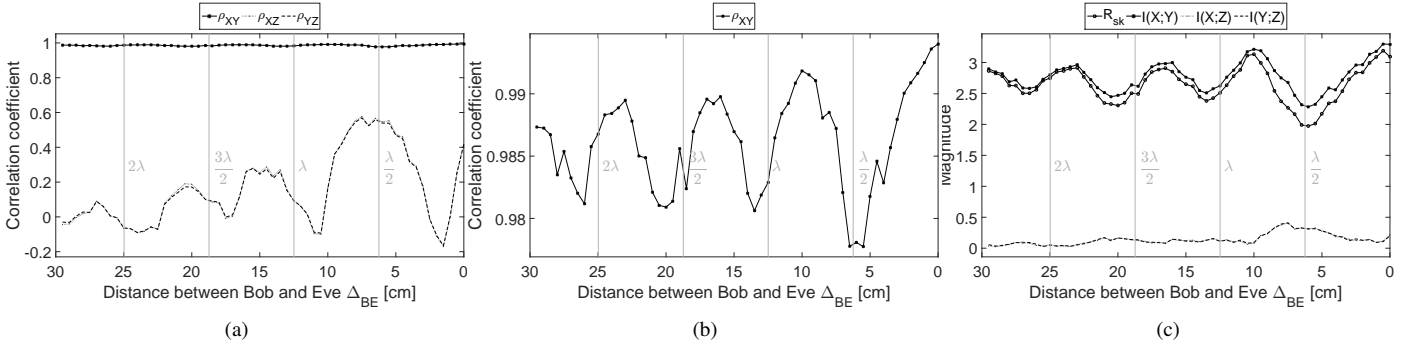


Fig. 12. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 1.

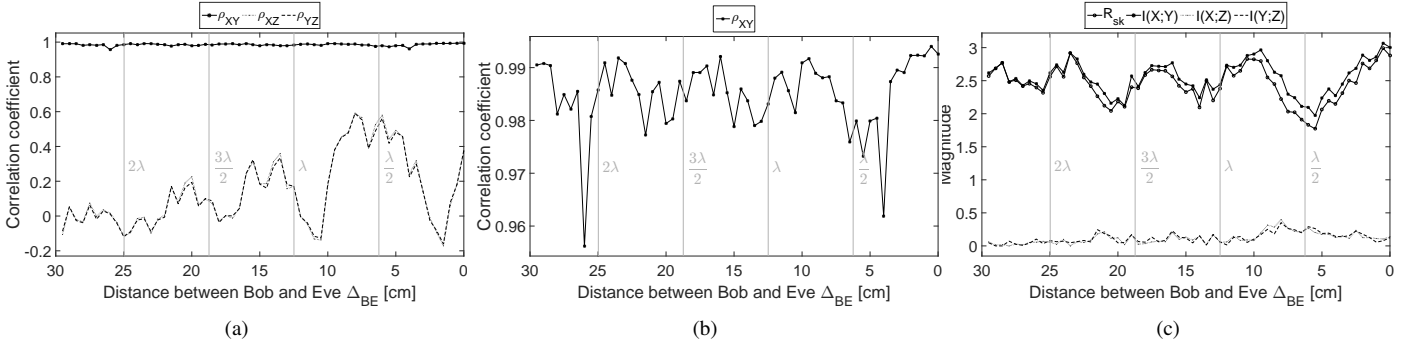


Fig. 13. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 1.

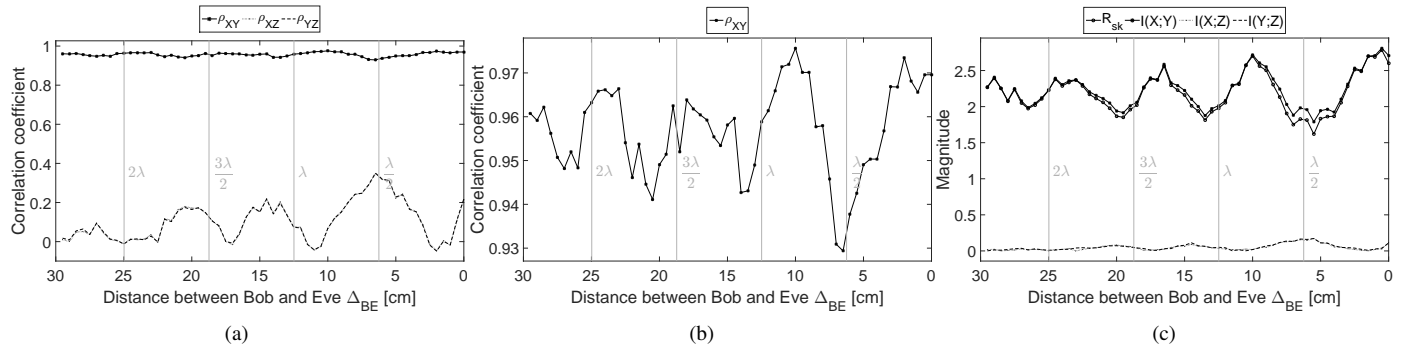


Fig. 14. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 1.

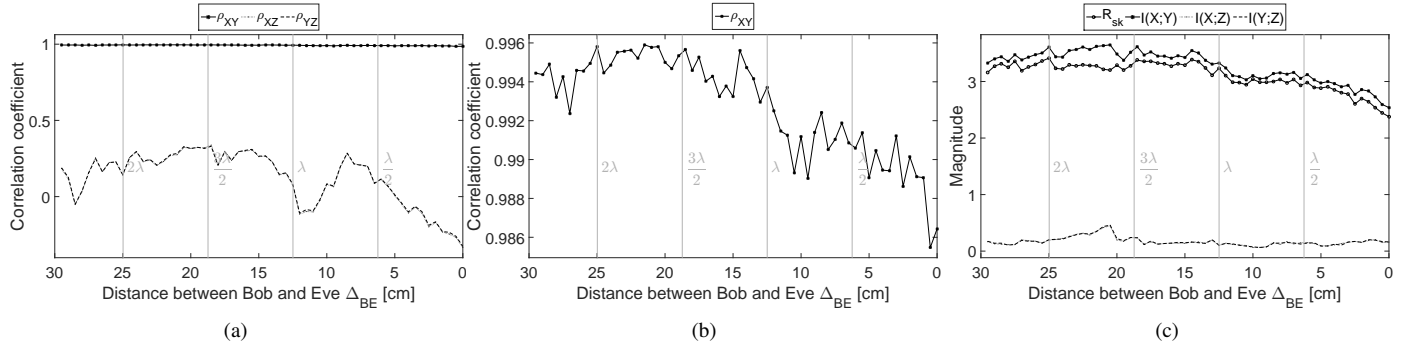


Fig. 15. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 2.

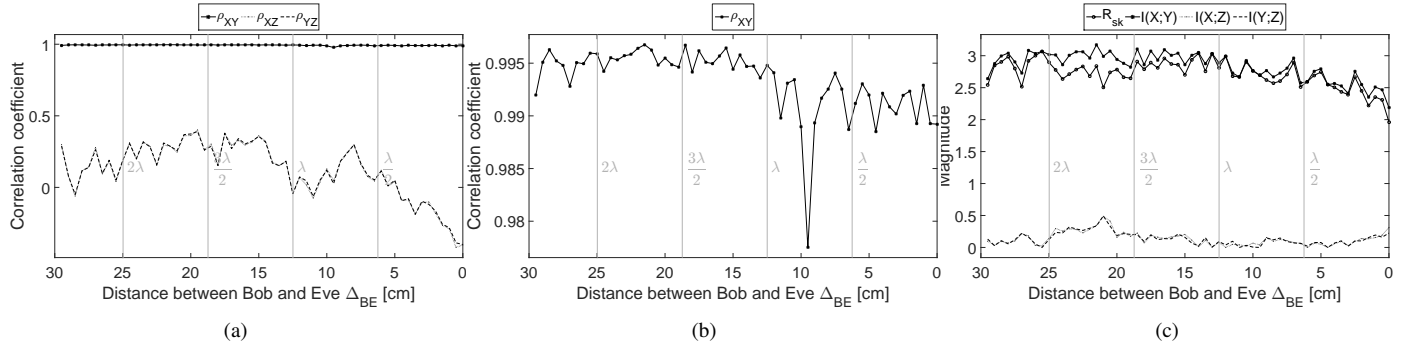


Fig. 16. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 2.

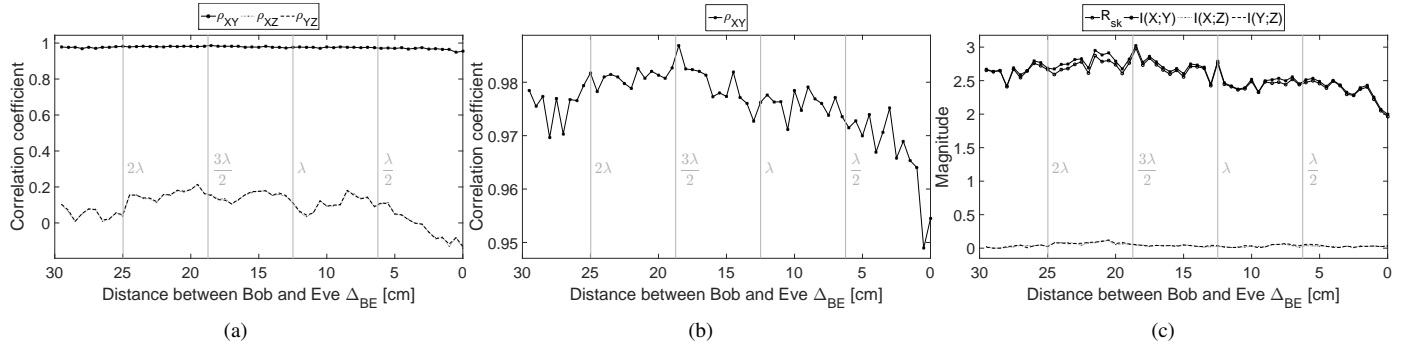


Fig. 17. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 2.

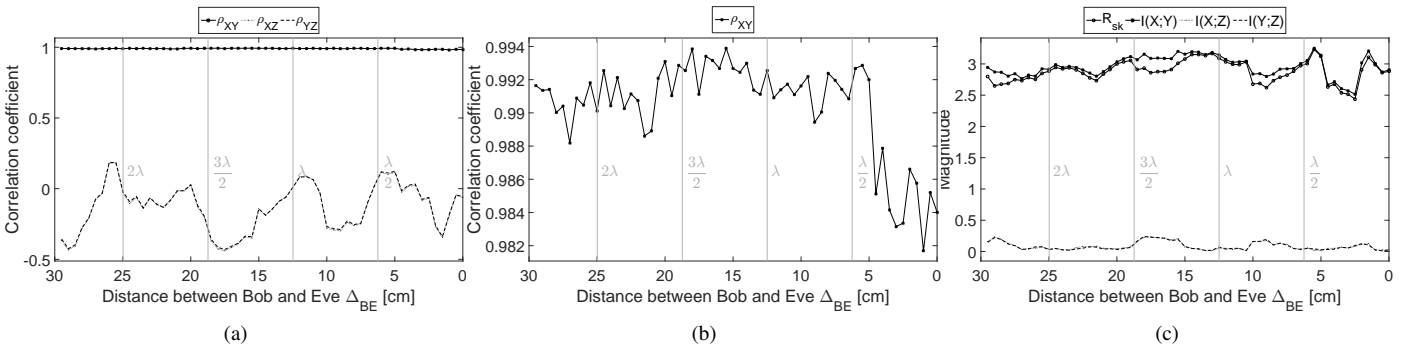


Fig. 18. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 3.

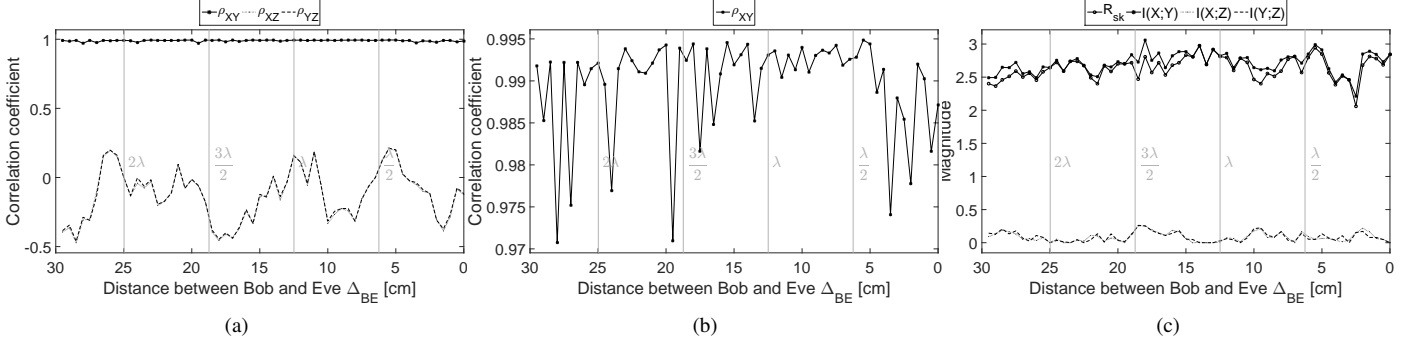


Fig. 19. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 3.

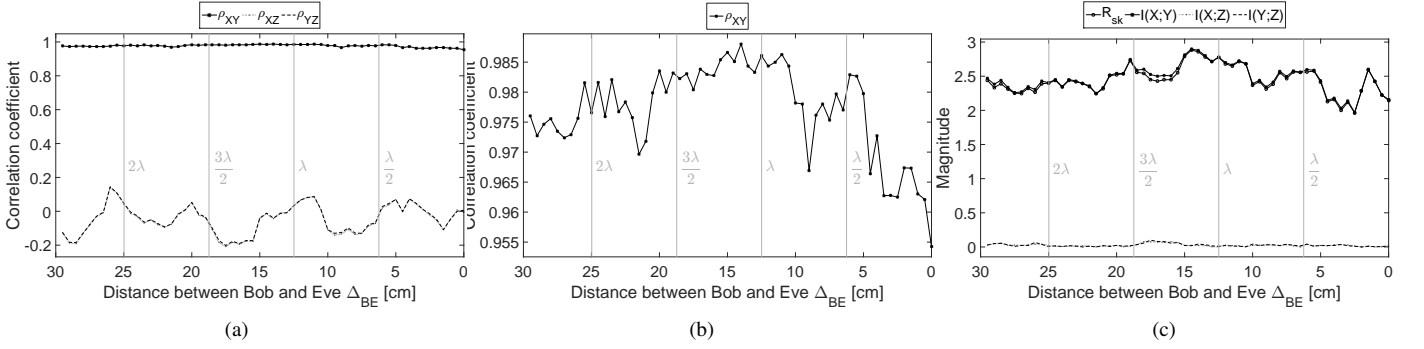


Fig. 20. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 3.

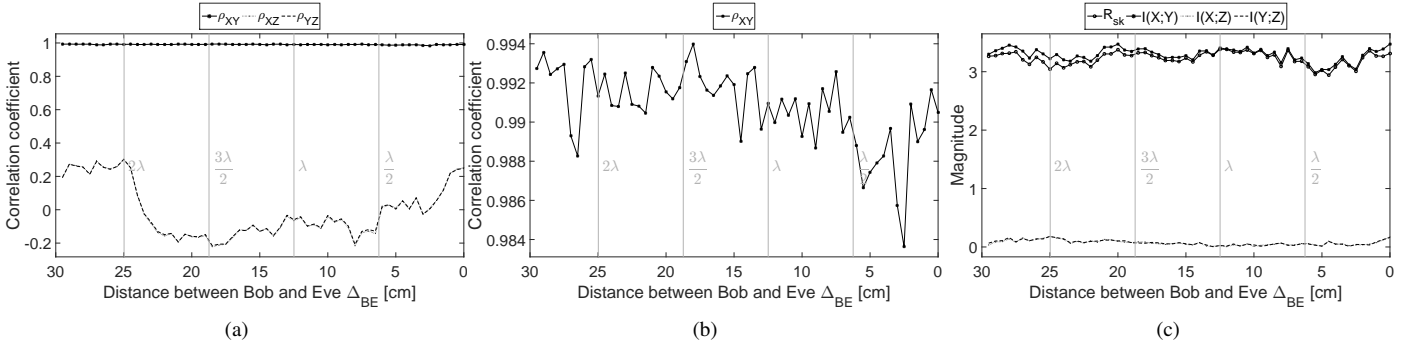


Fig. 21. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 4.

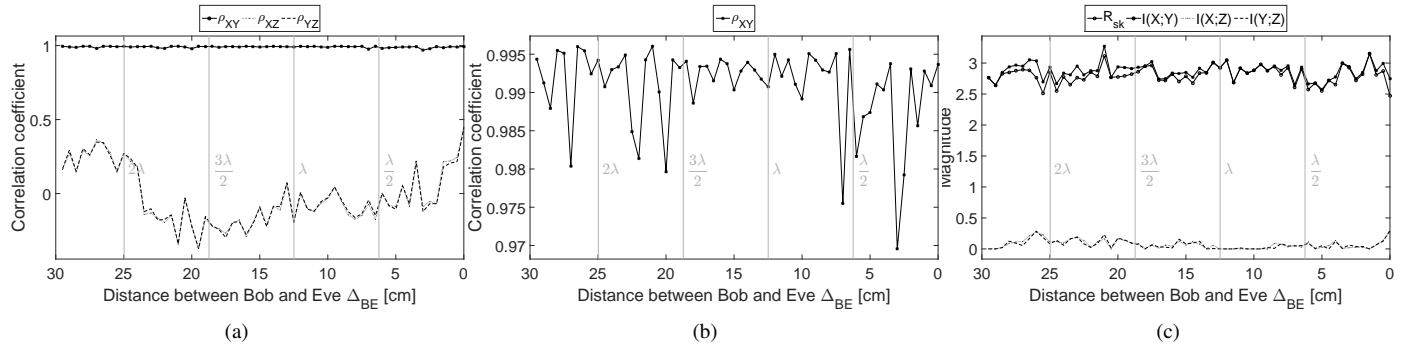


Fig. 22. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 4.

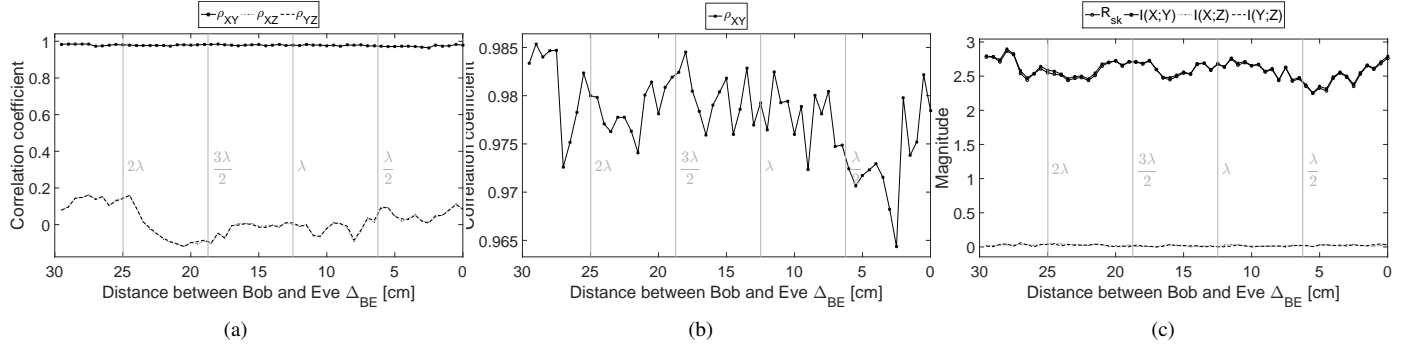


Fig. 23. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 4.

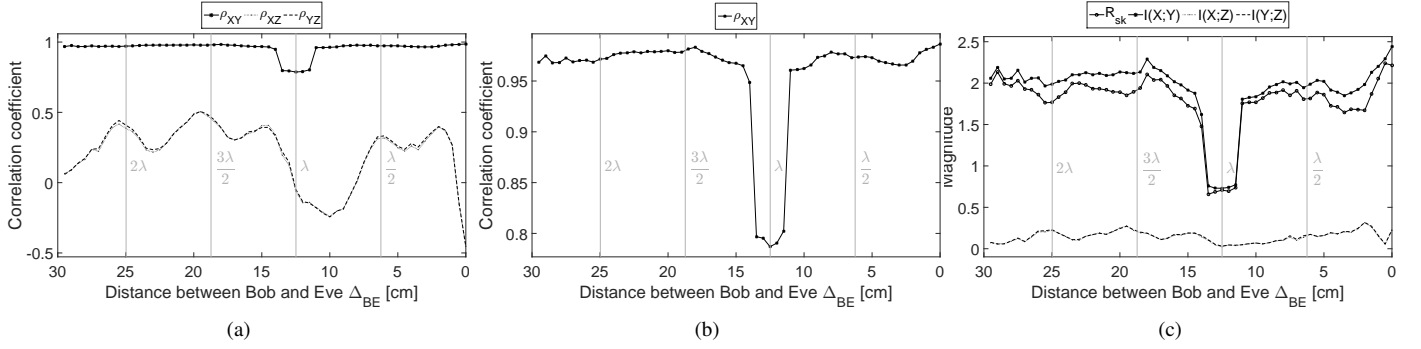


Fig. 24. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 5.

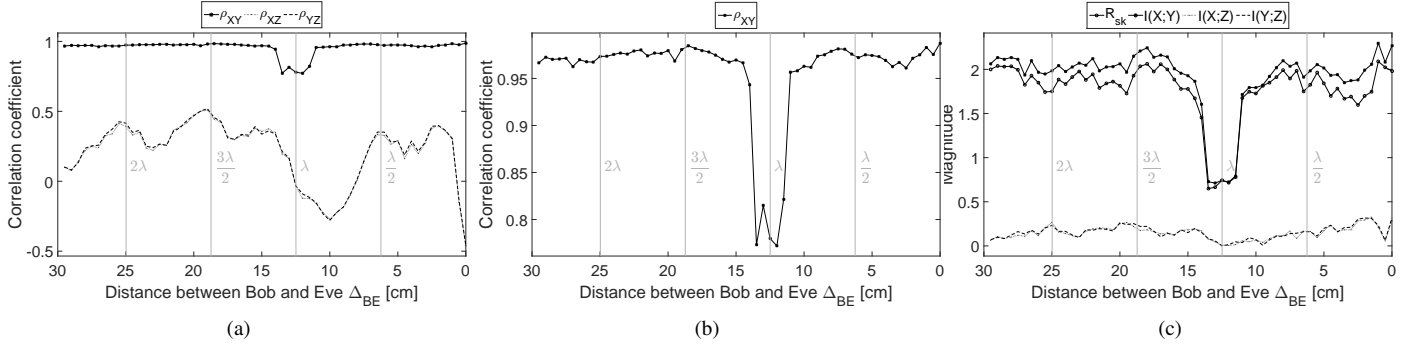


Fig. 25. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 5.

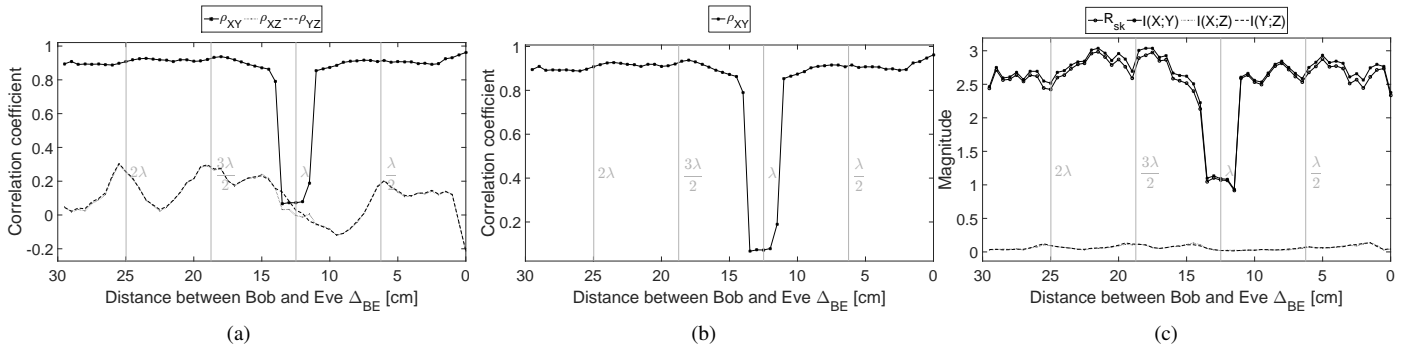


Fig. 26. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 5.

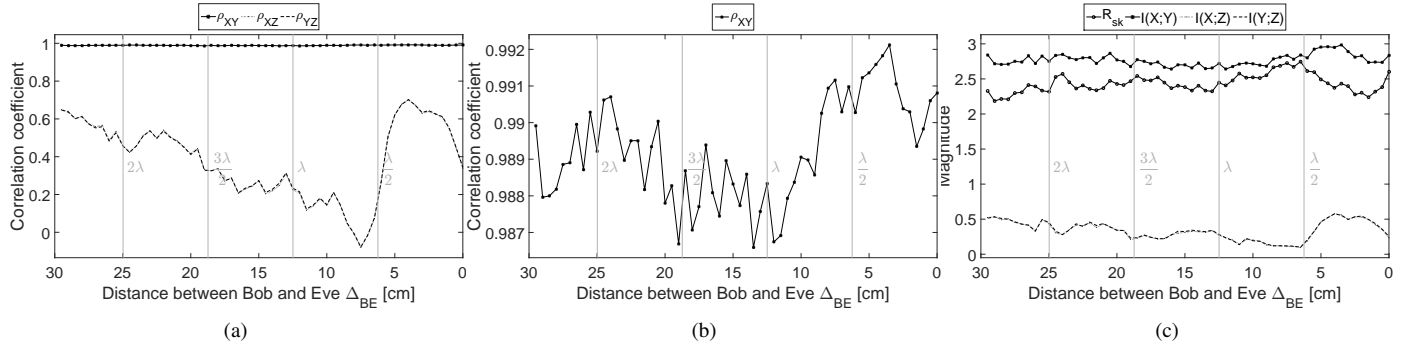


Fig. 27. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 6.

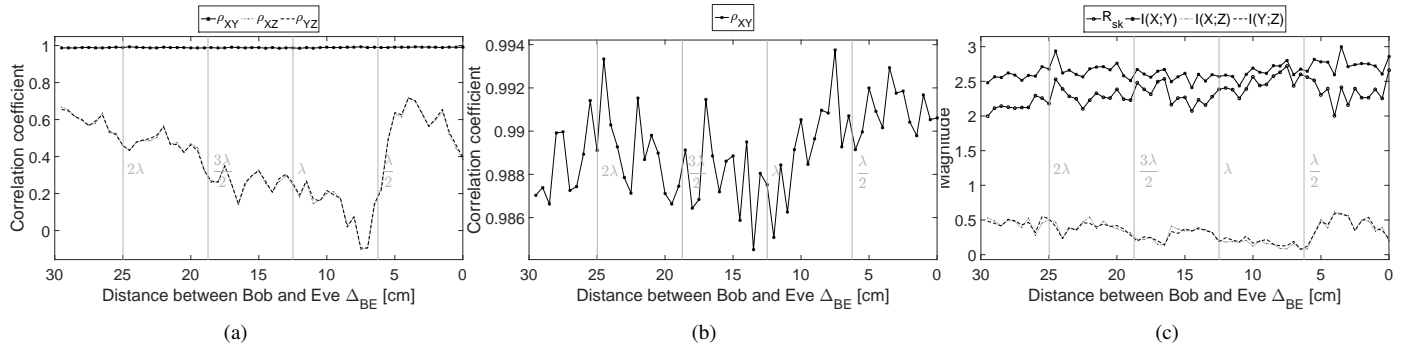


Fig. 28. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 6.

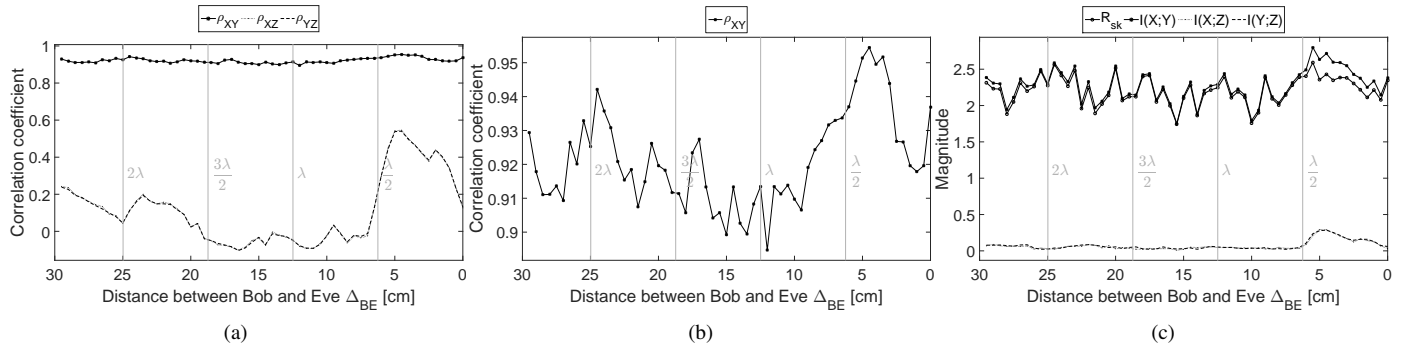


Fig. 29. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 6.

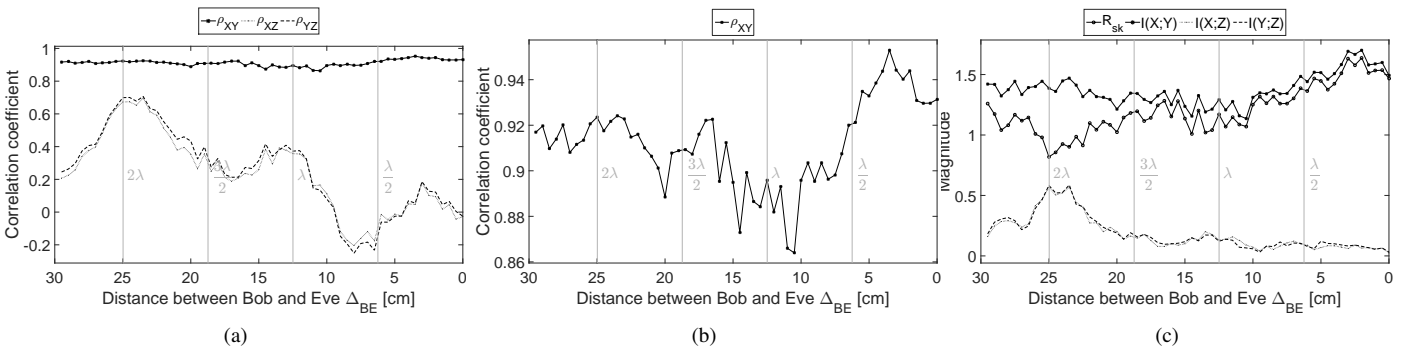


Fig. 30. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 7.

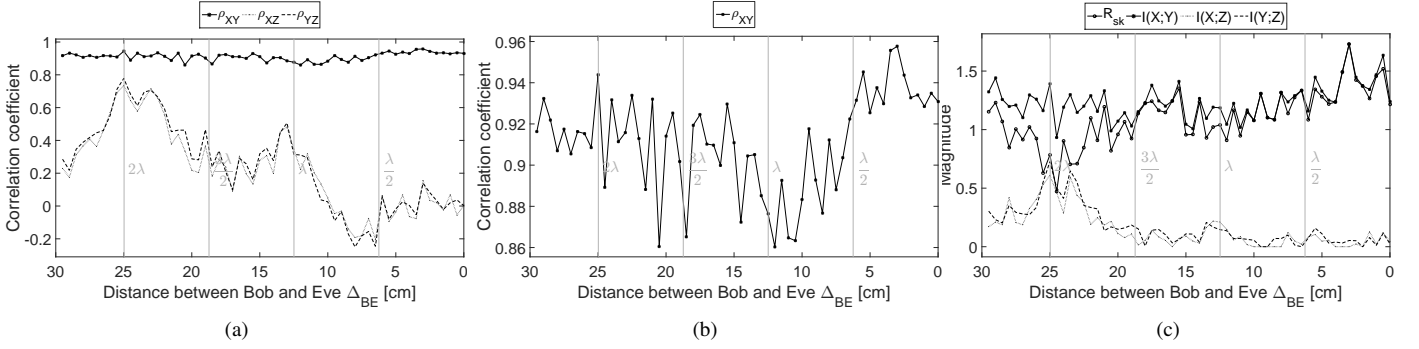


Fig. 31. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 7.

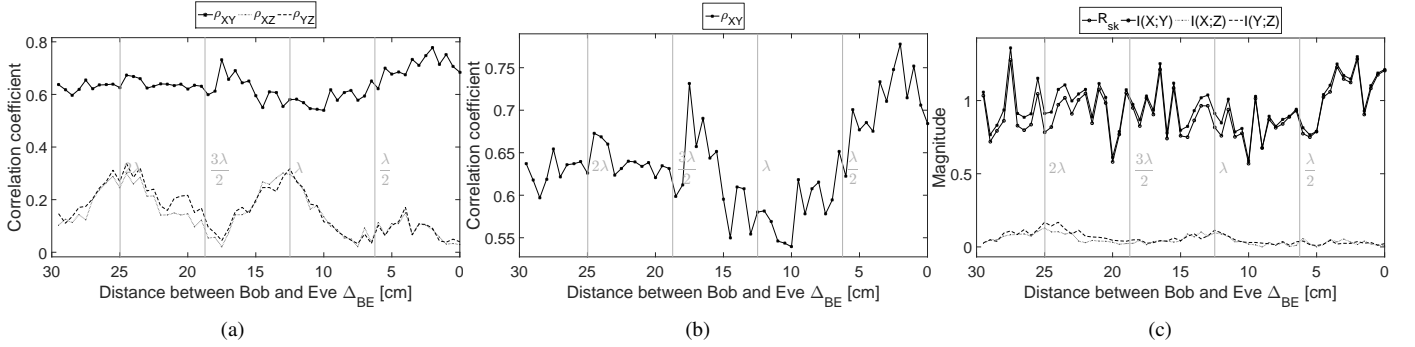


Fig. 32. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 7.

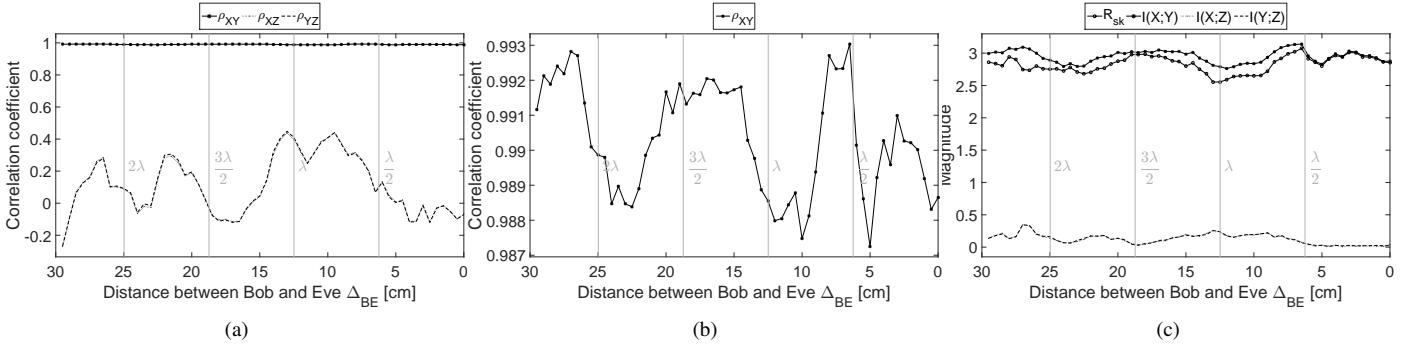


Fig. 33. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 8.

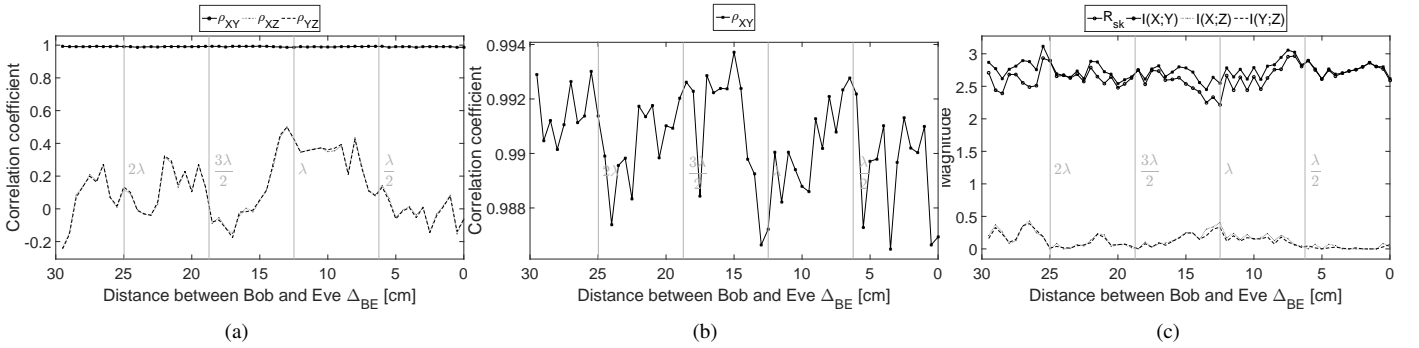


Fig. 34. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 8.

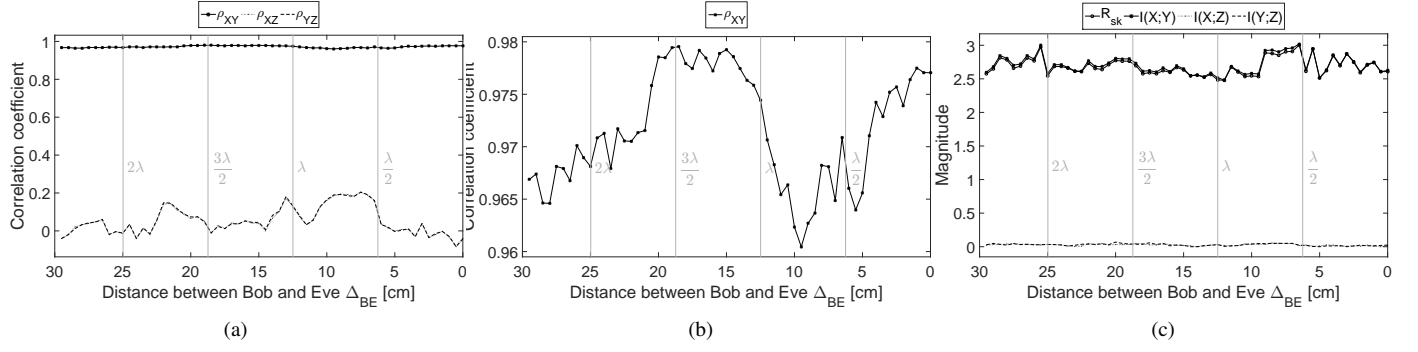


Fig. 35. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 8.

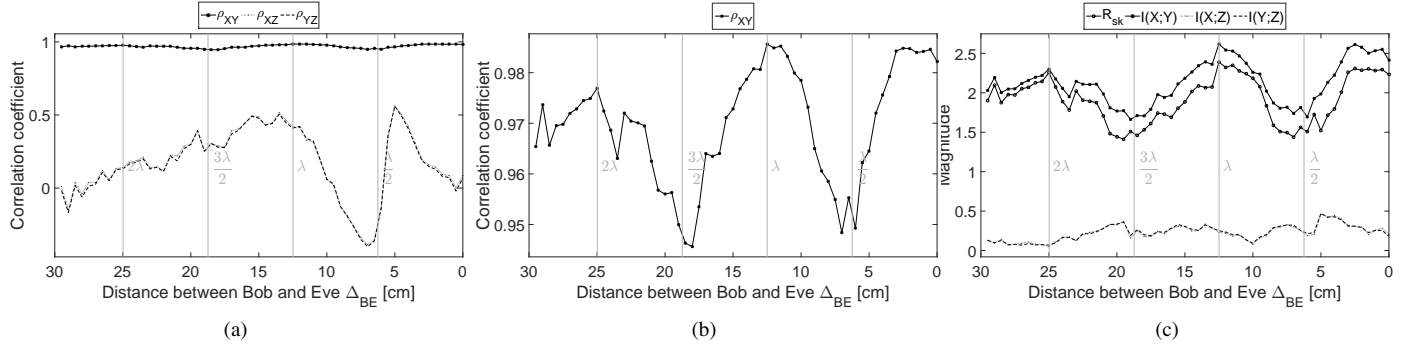


Fig. 36. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 9.

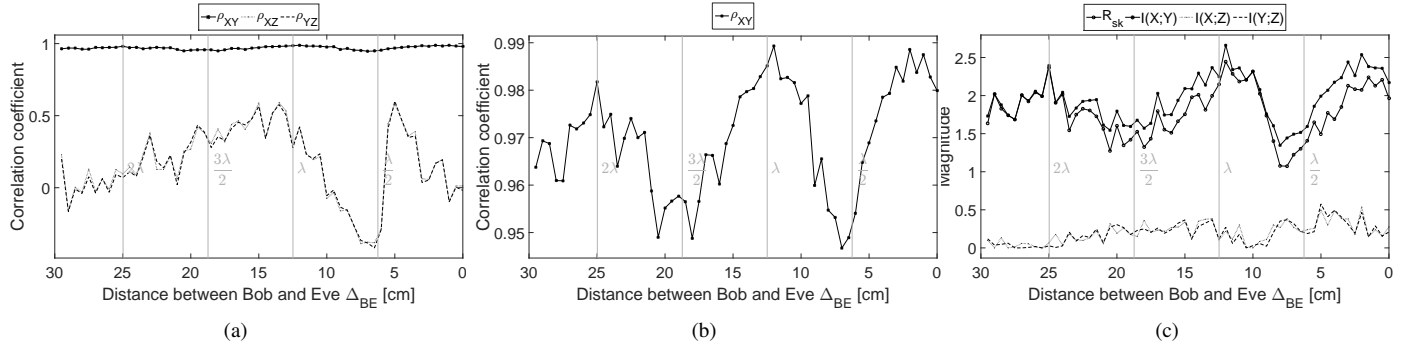


Fig. 37. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 9.

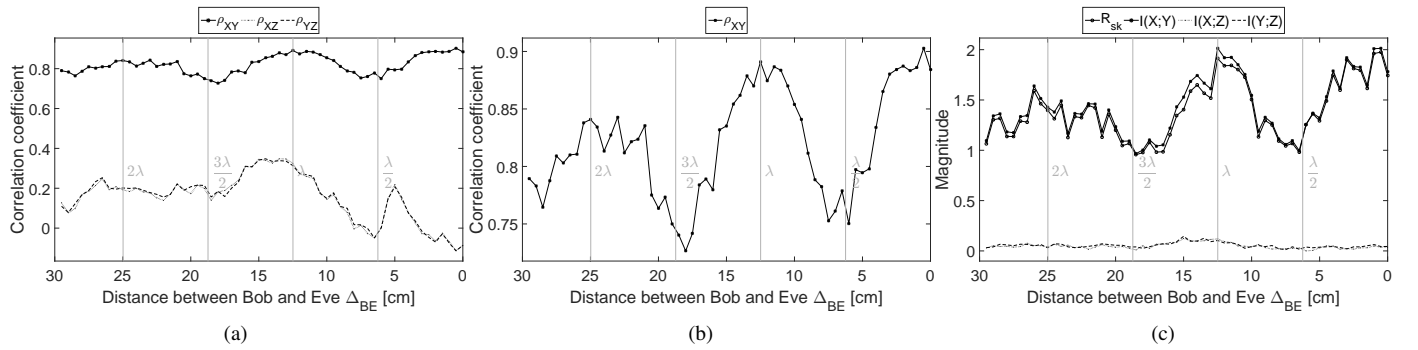


Fig. 38. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 9.

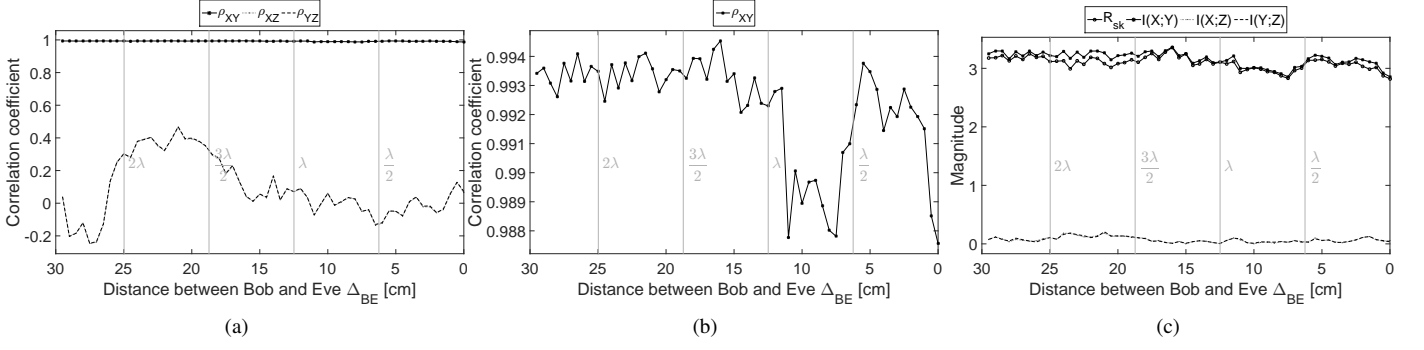


Fig. 39. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 10.

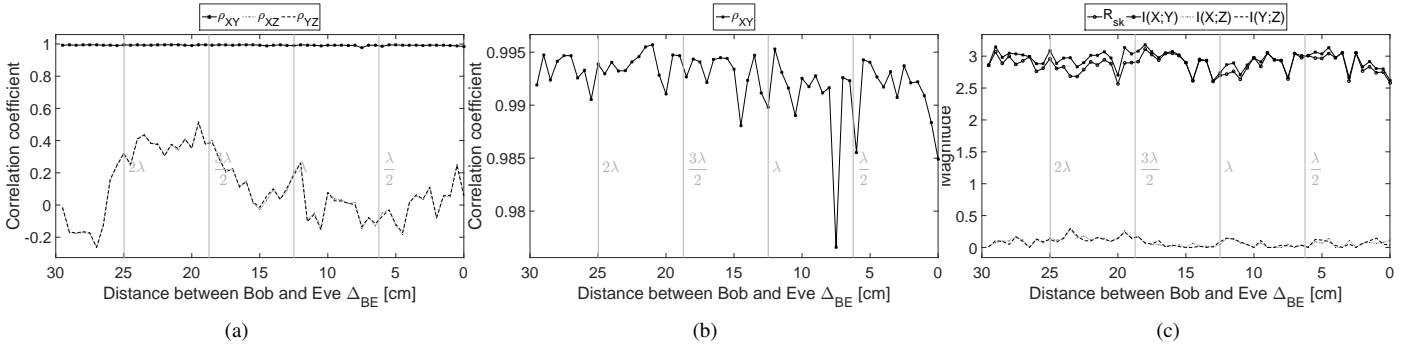


Fig. 40. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 10.

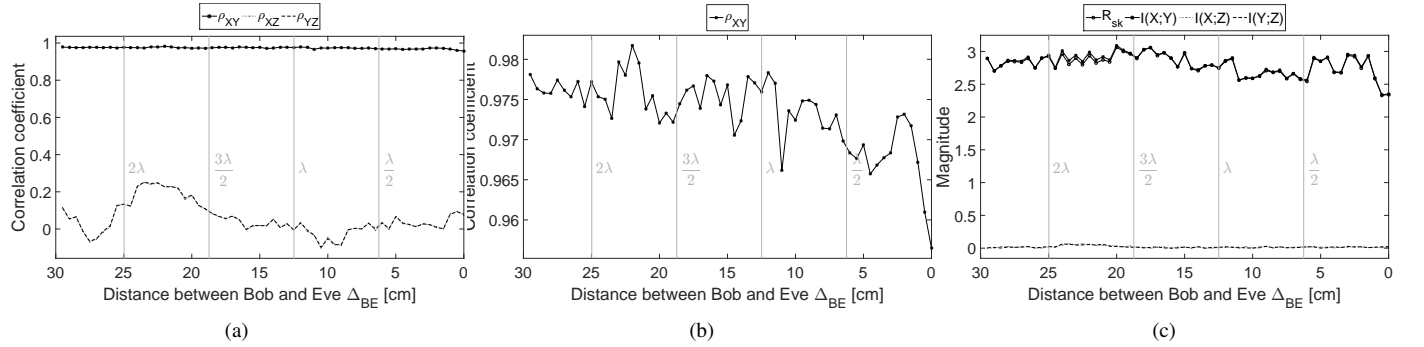


Fig. 41. Evaluation results of v_k^{dc} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 10.

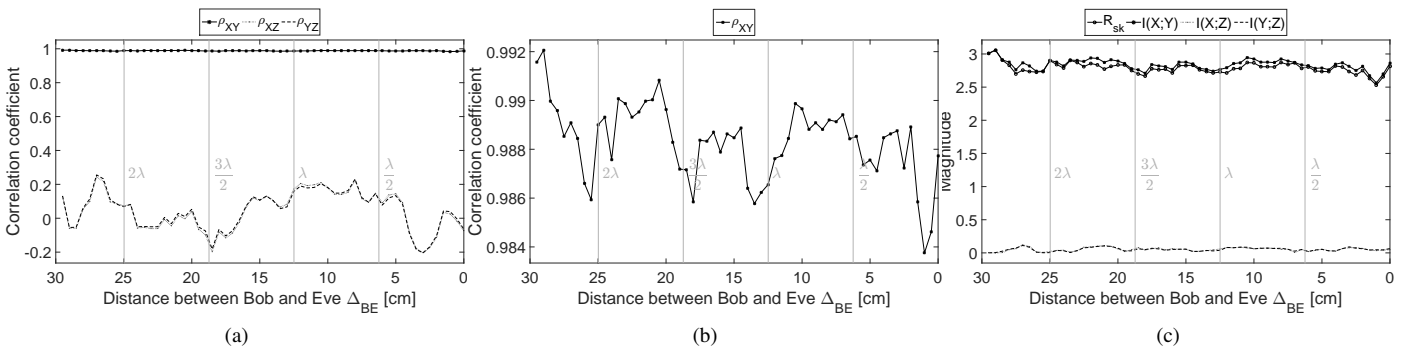


Fig. 42. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 11.

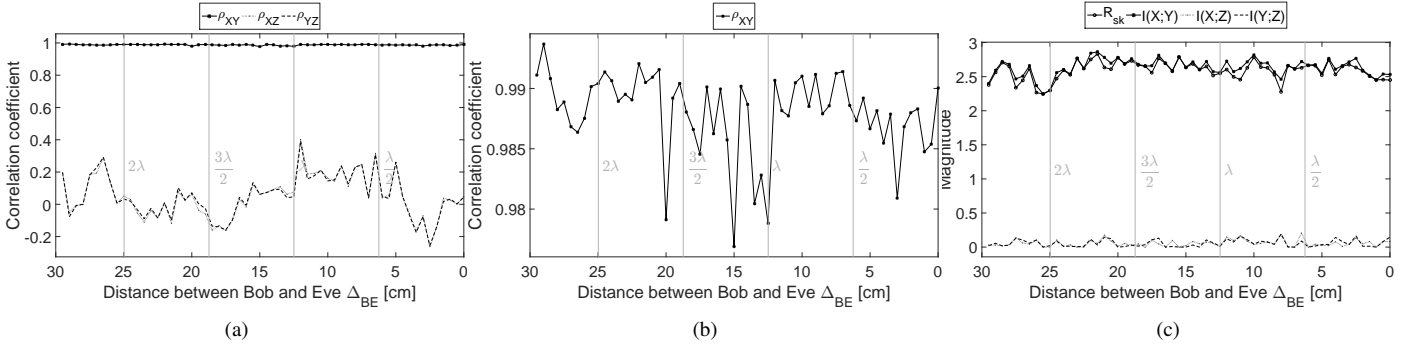


Fig. 43. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 11.

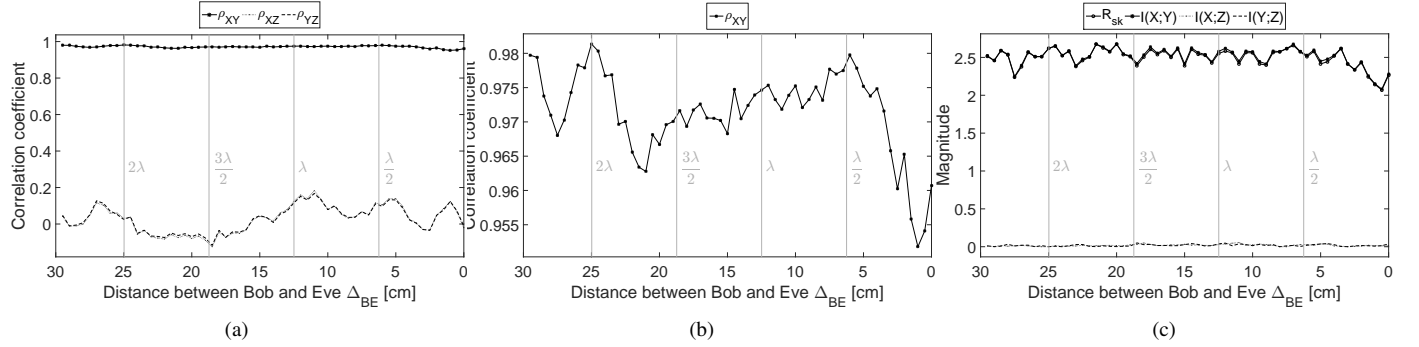


Fig. 44. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 11.

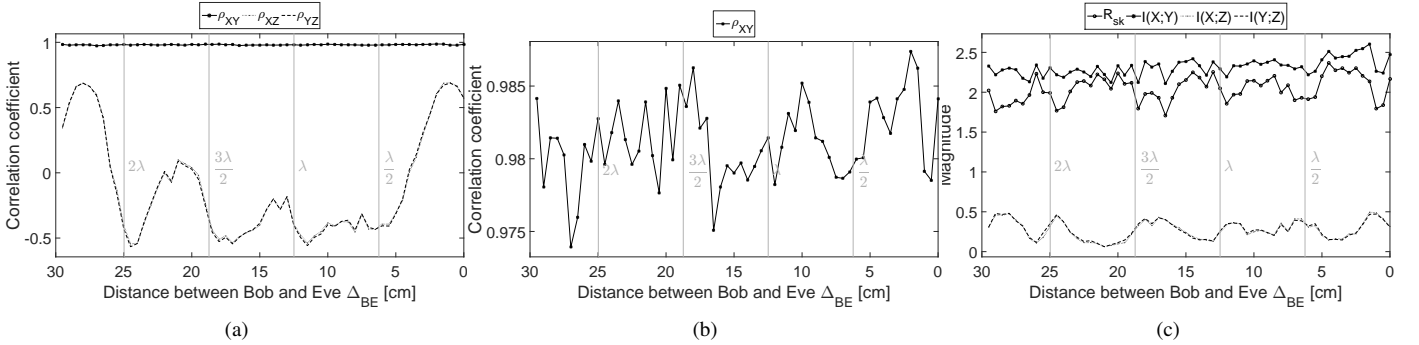


Fig. 45. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 12.

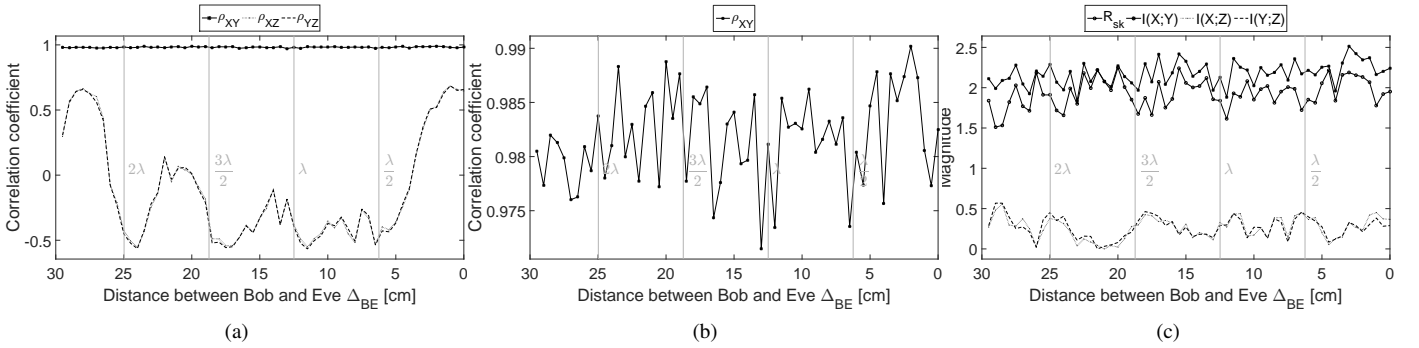


Fig. 46. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 12.

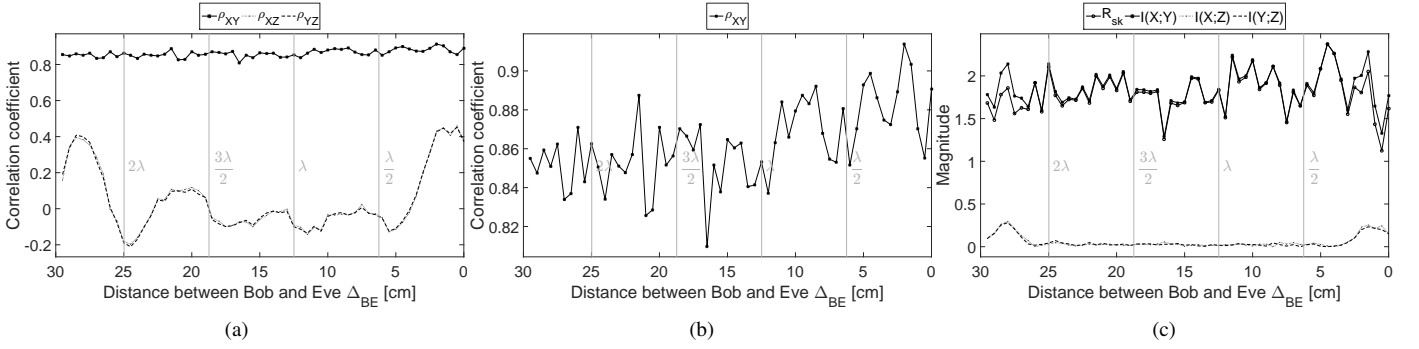


Fig. 47. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 12.

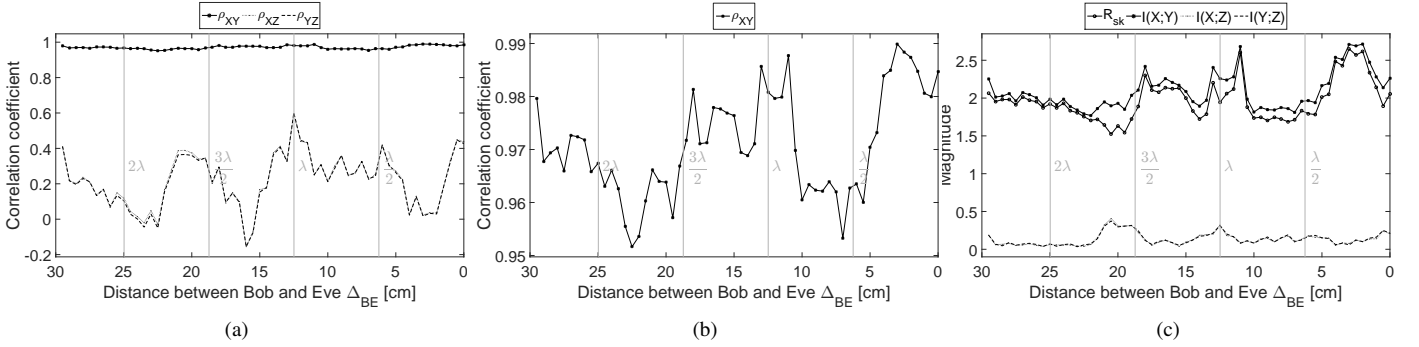


Fig. 48. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 13.

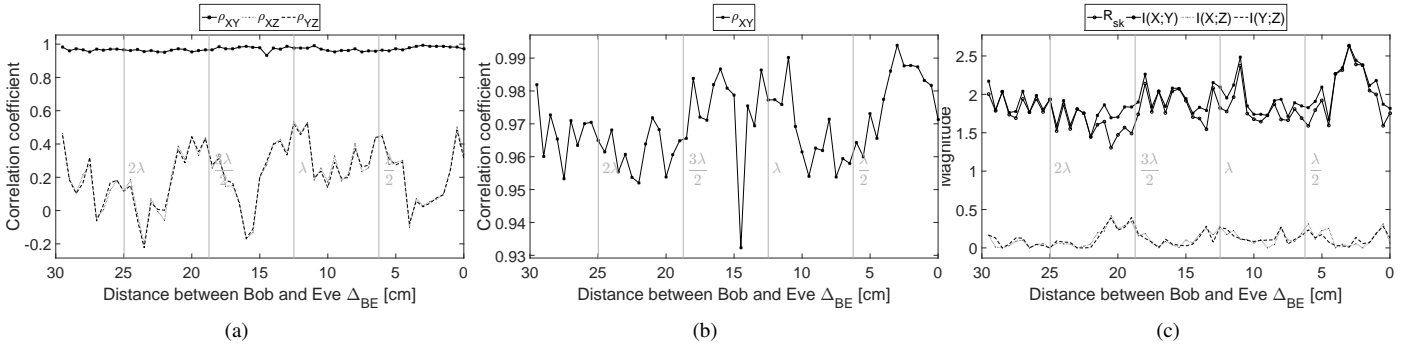


Fig. 49. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 13.

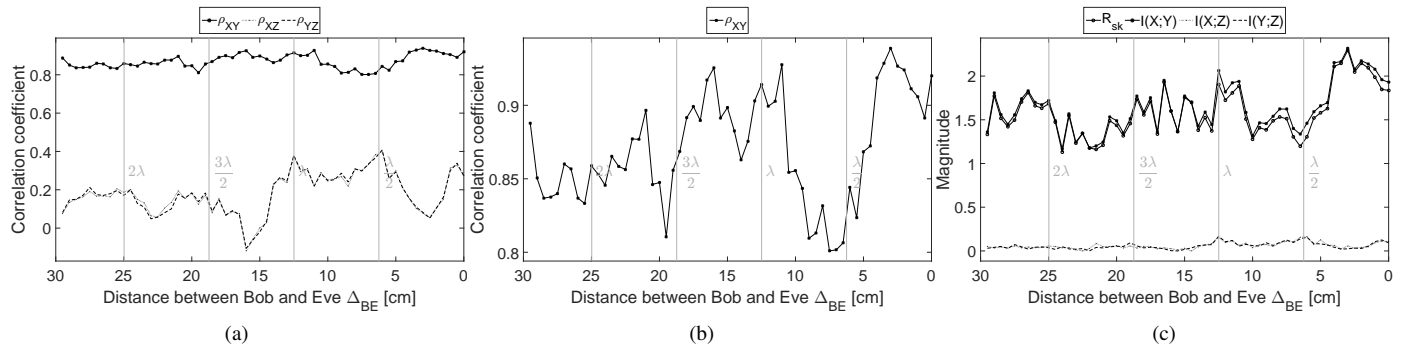


Fig. 50. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 13.

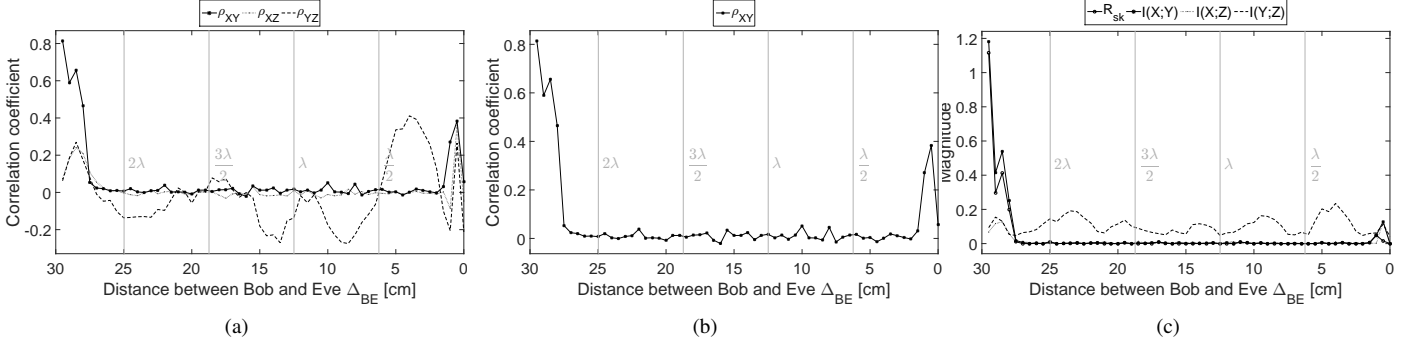


Fig. 51. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 14.

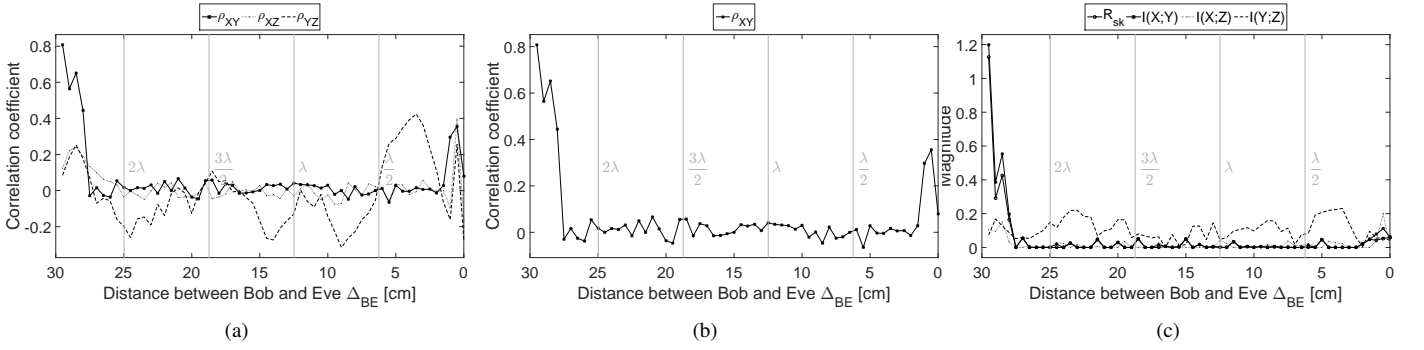


Fig. 52. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 14.

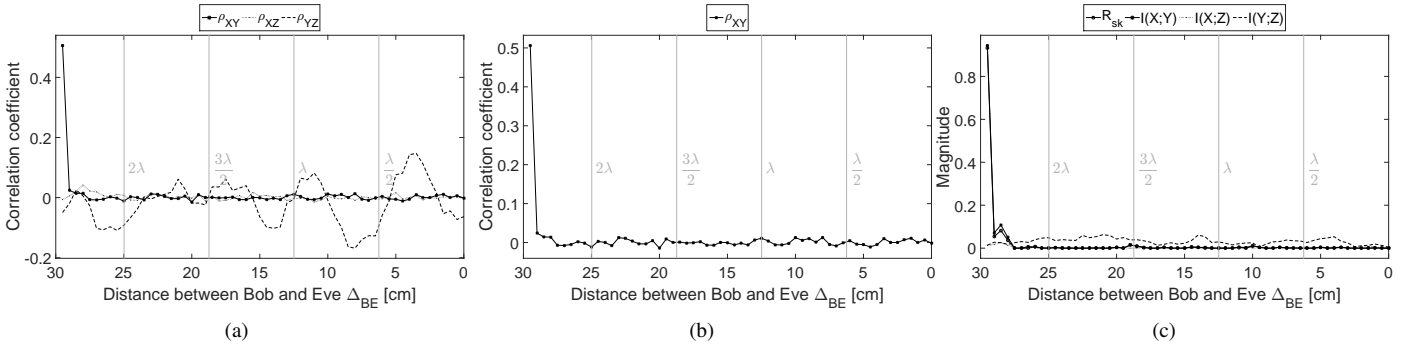


Fig. 53. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 14.

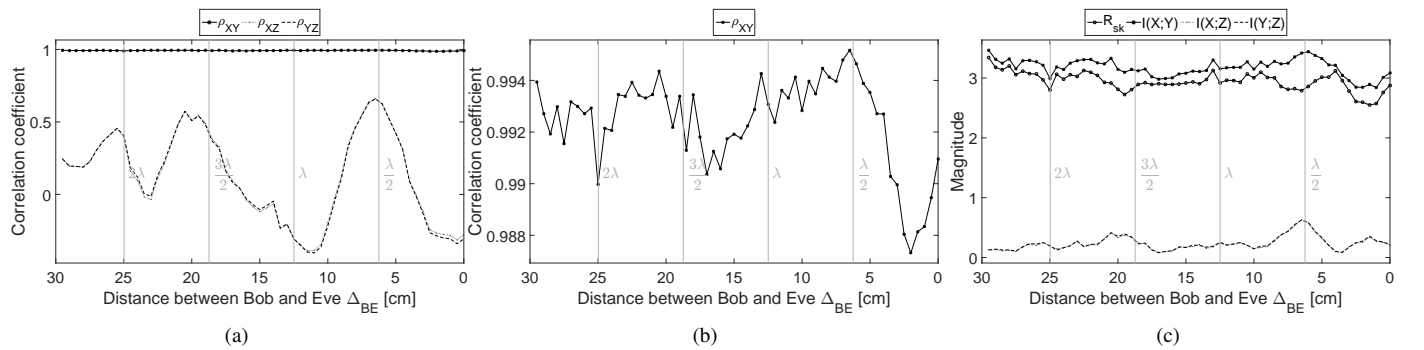


Fig. 54. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 15.

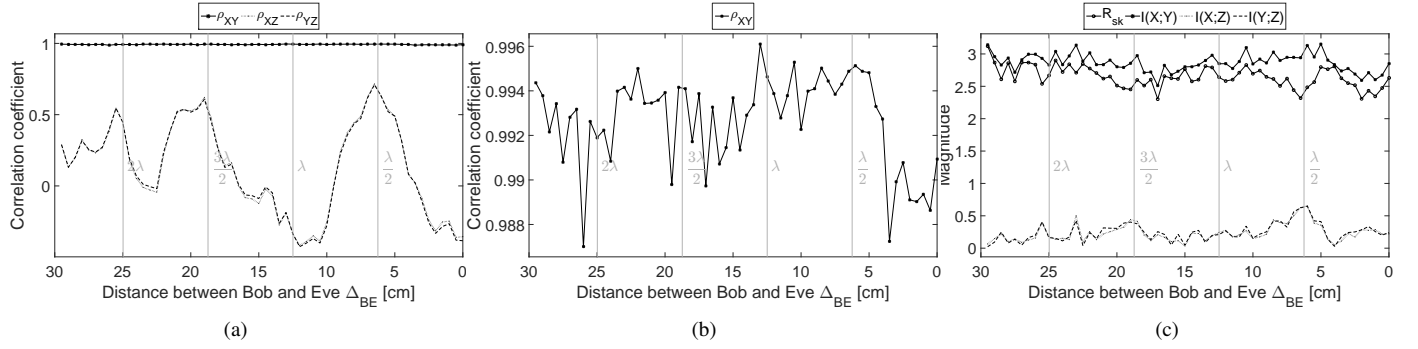


Fig. 55. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 15.

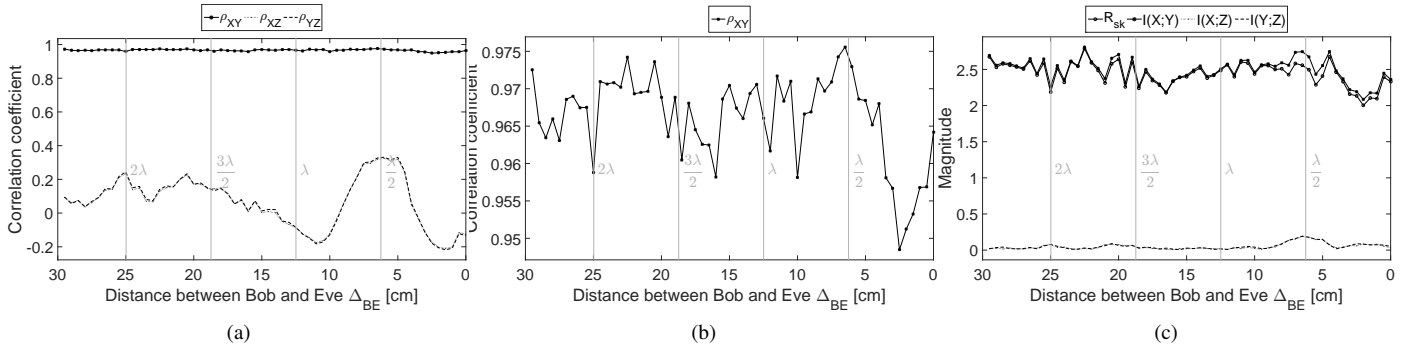


Fig. 56. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 15.

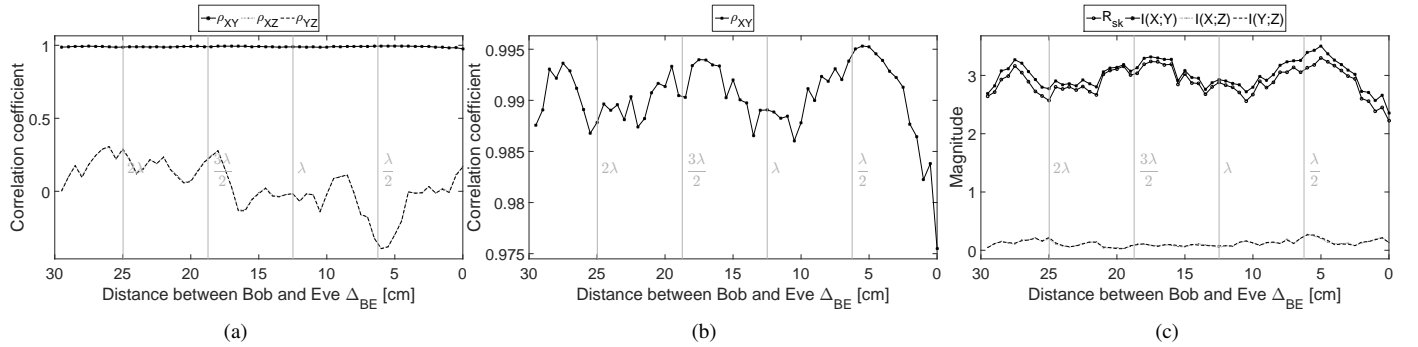


Fig. 57. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 16.

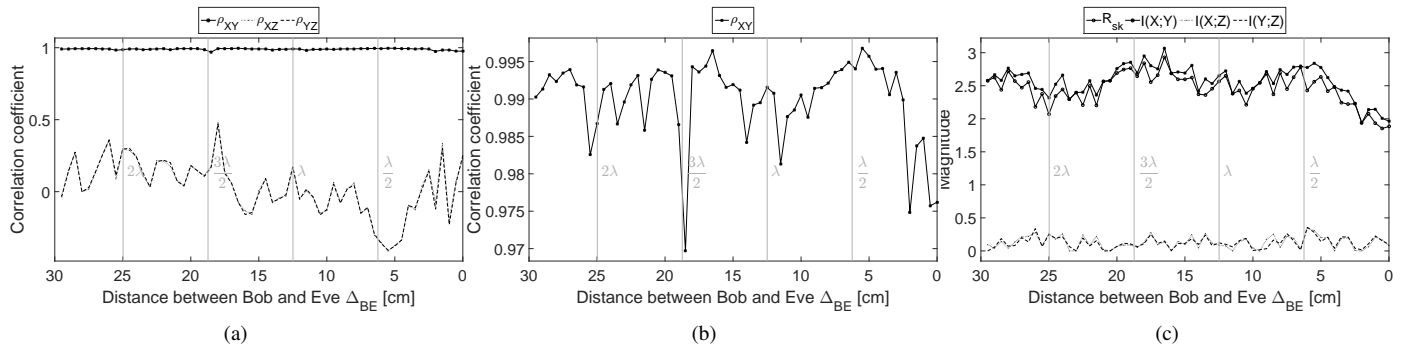


Fig. 58. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 16.

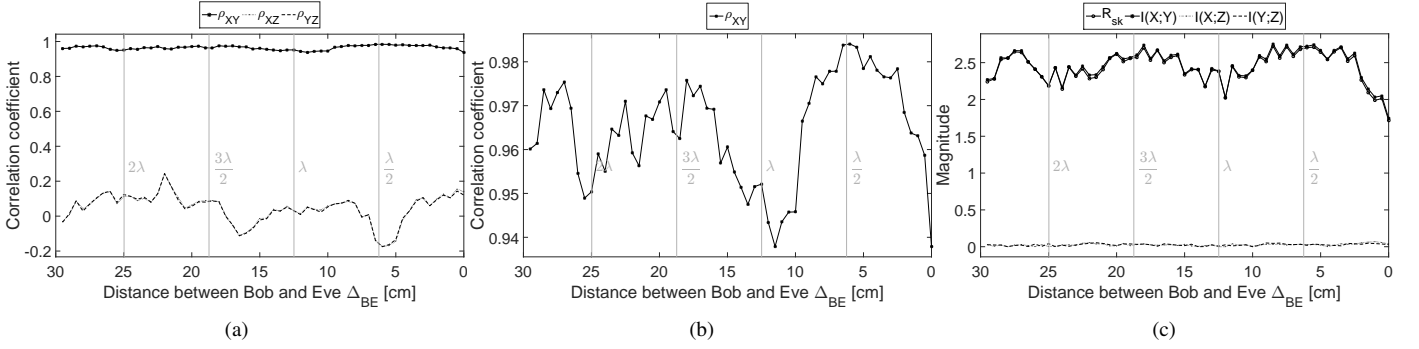


Fig. 59. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 16.

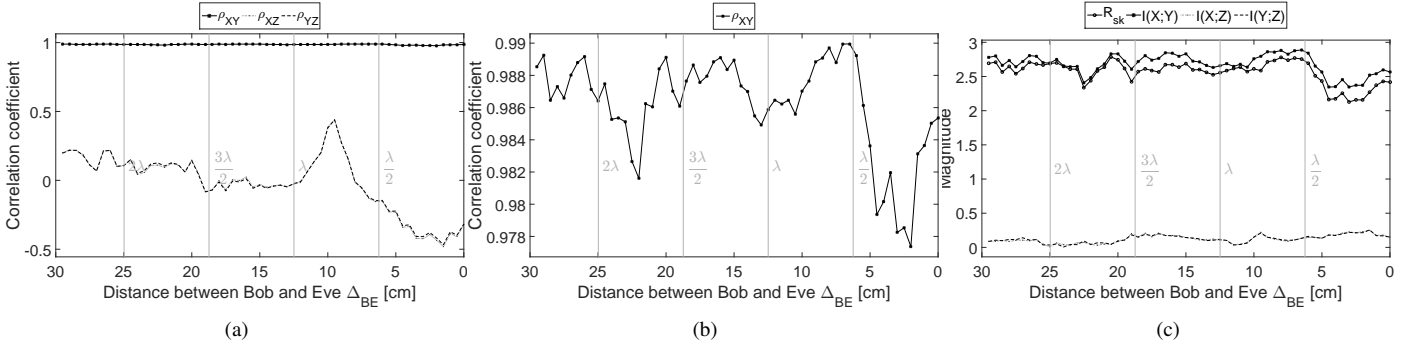


Fig. 60. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 17.

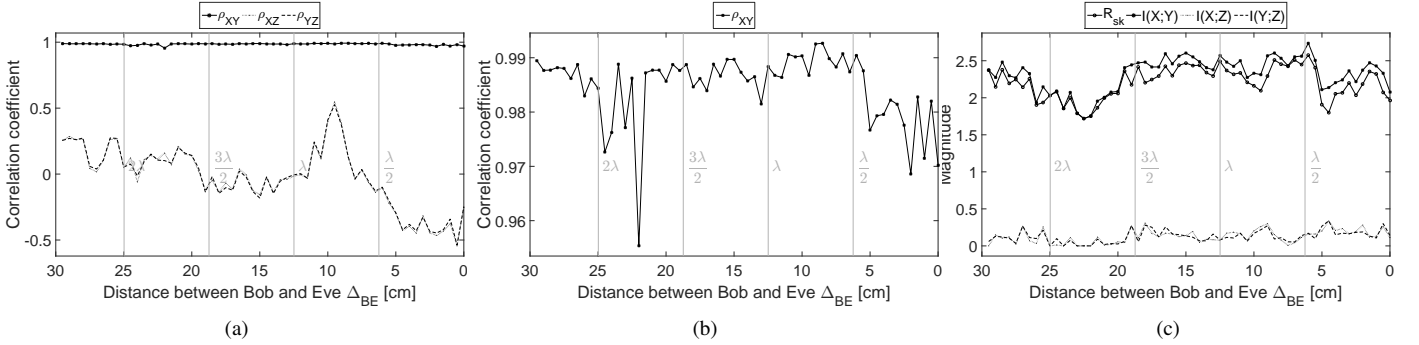


Fig. 61. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 17.

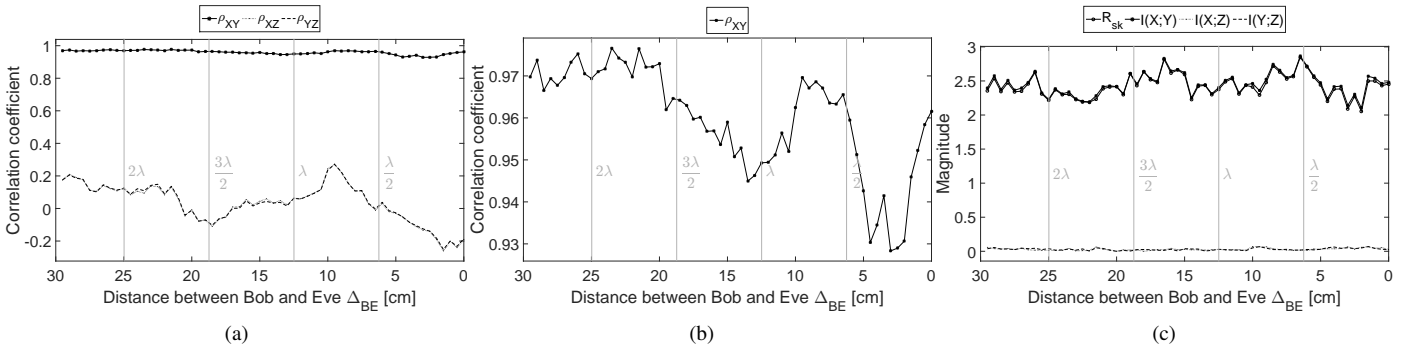


Fig. 62. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 17.

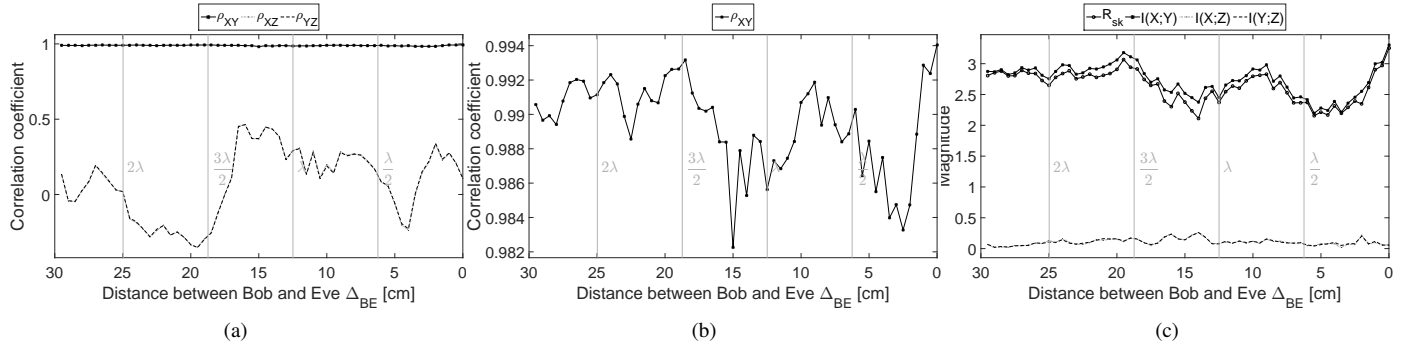


Fig. 63. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 18.

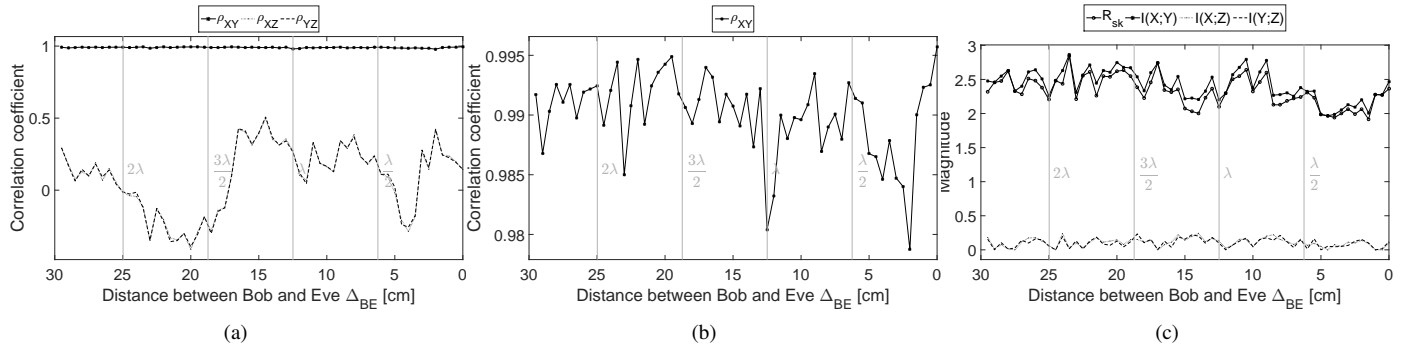


Fig. 64. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 18.

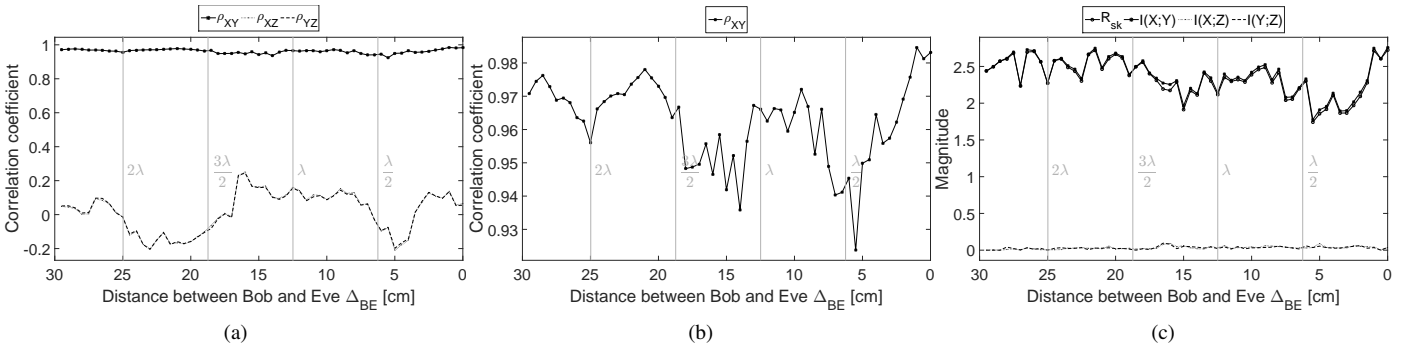


Fig. 65. Evaluation results of v_k^{dc} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 18.

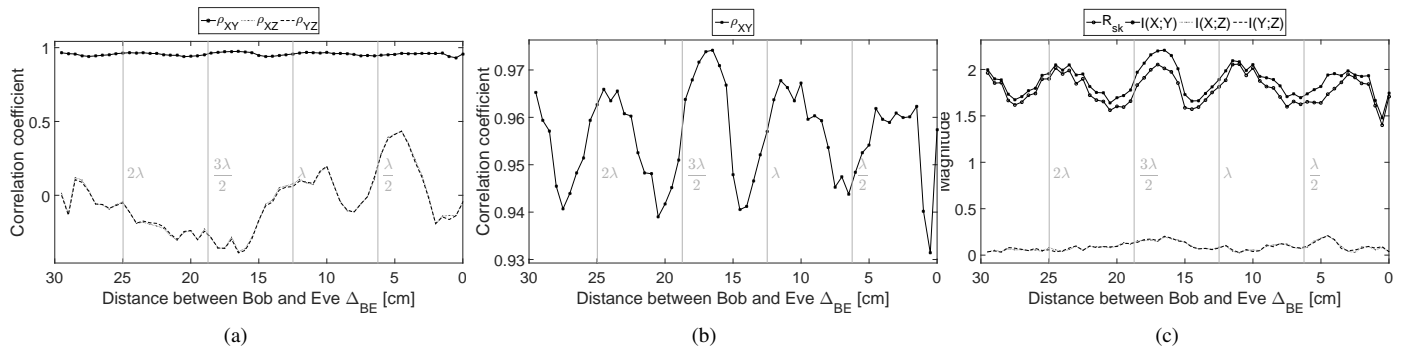


Fig. 66. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 19.

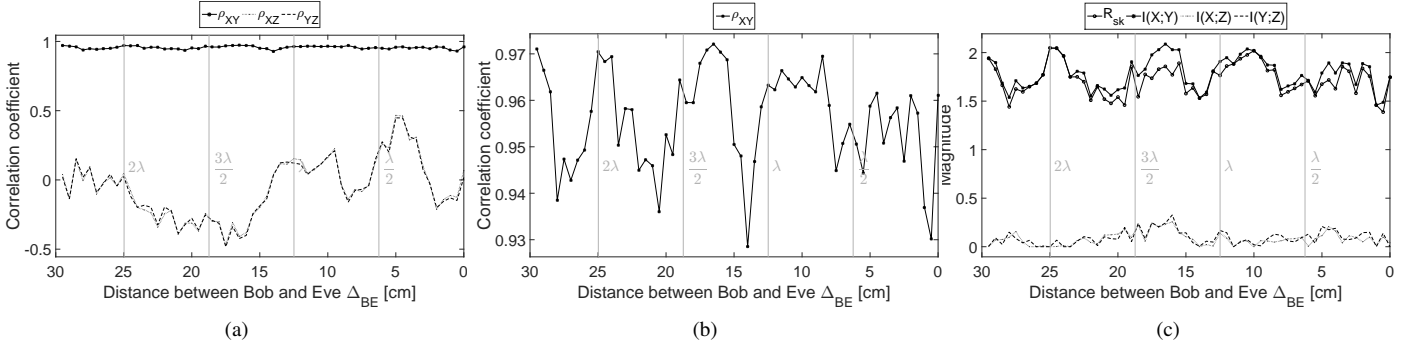


Fig. 67. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 19.

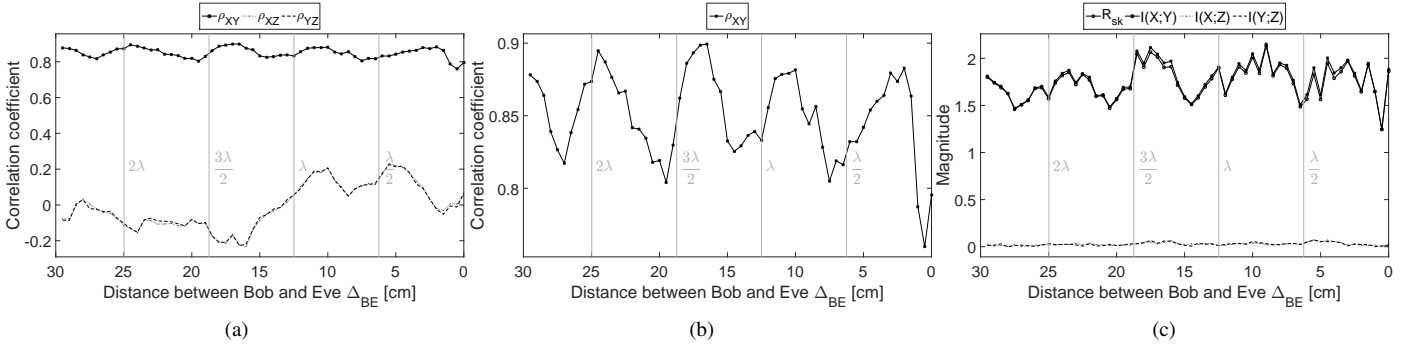


Fig. 68. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 19.

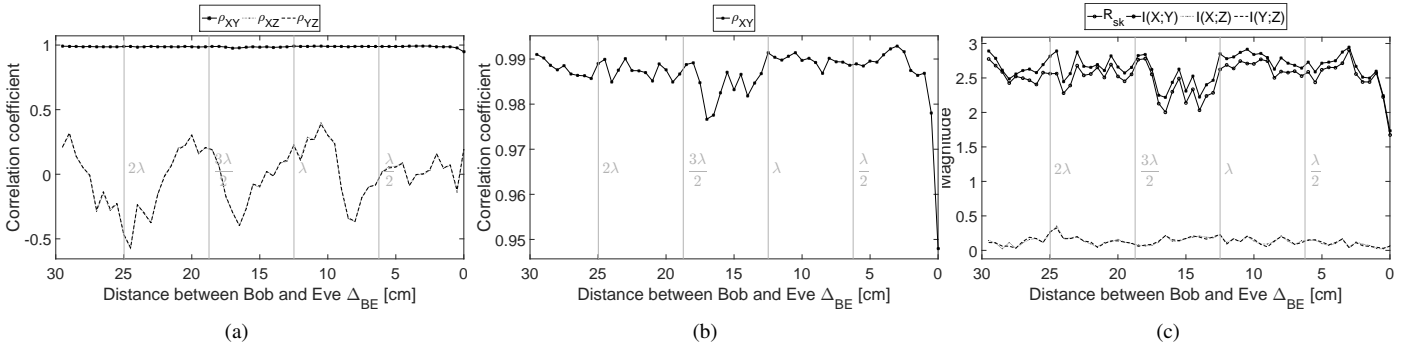


Fig. 69. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 20.

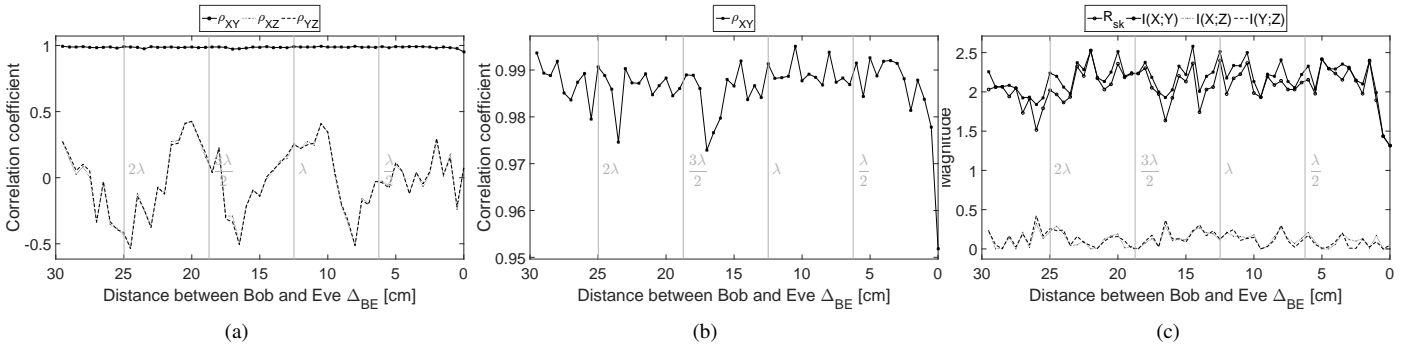


Fig. 70. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 20.

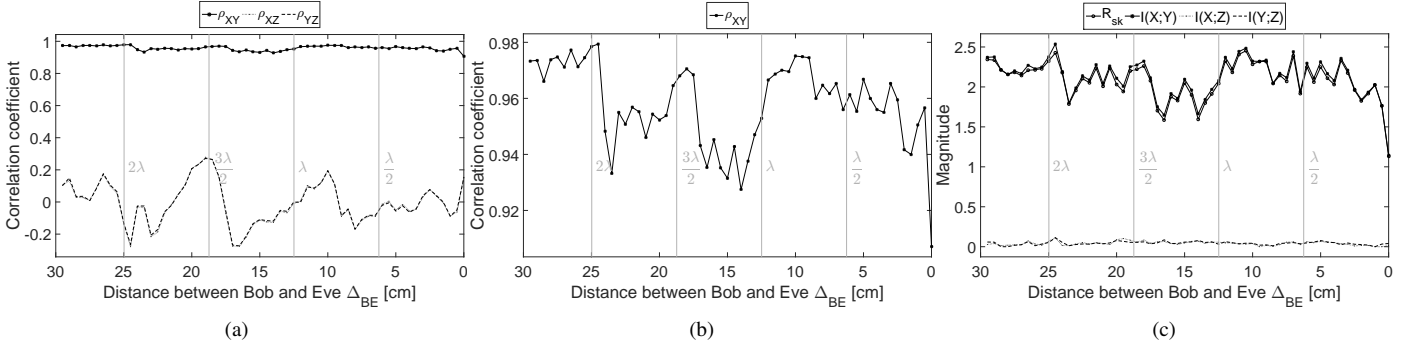


Fig. 71. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 20.

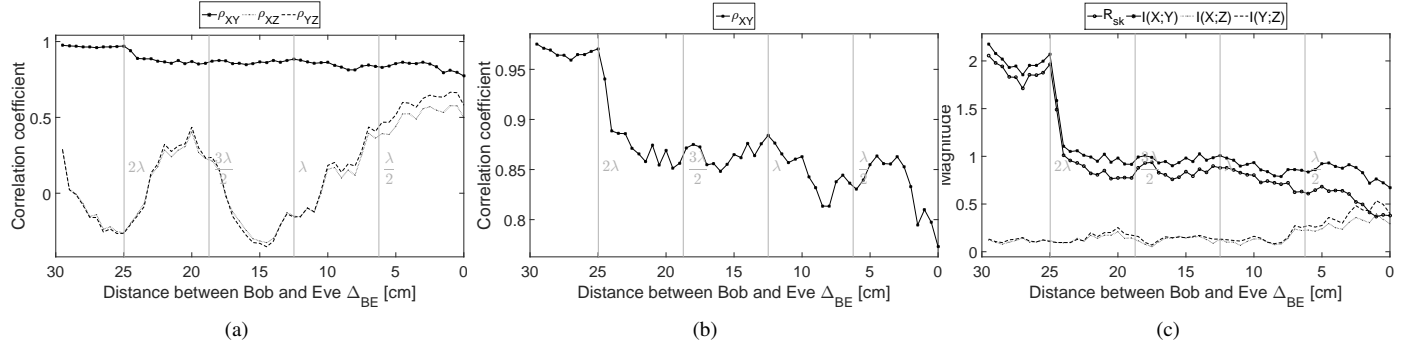


Fig. 72. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 21.

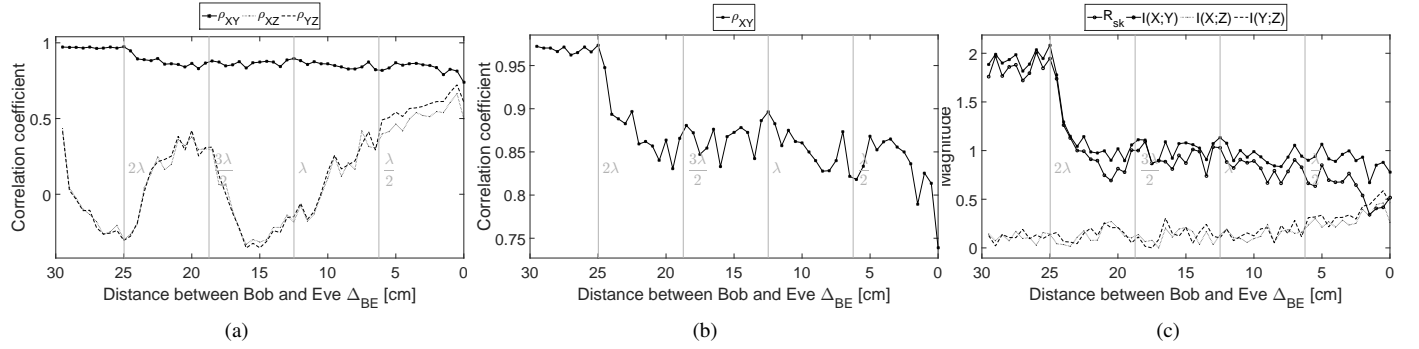


Fig. 73. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 21.

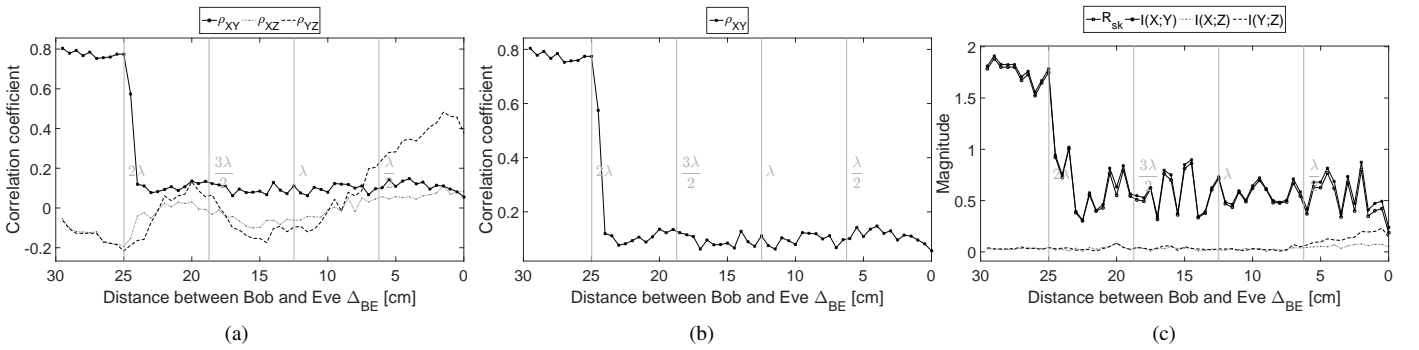


Fig. 74. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 21.

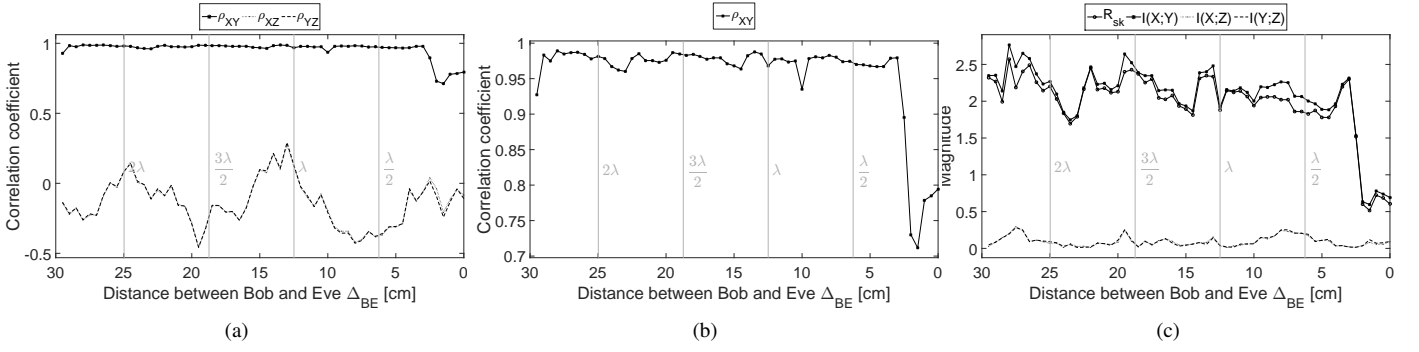


Fig. 75. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 22.

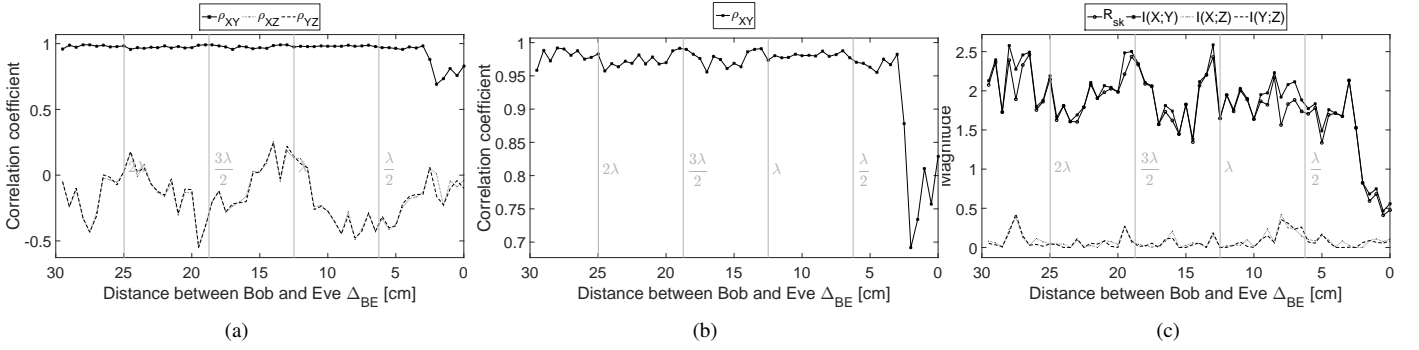


Fig. 76. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 22.

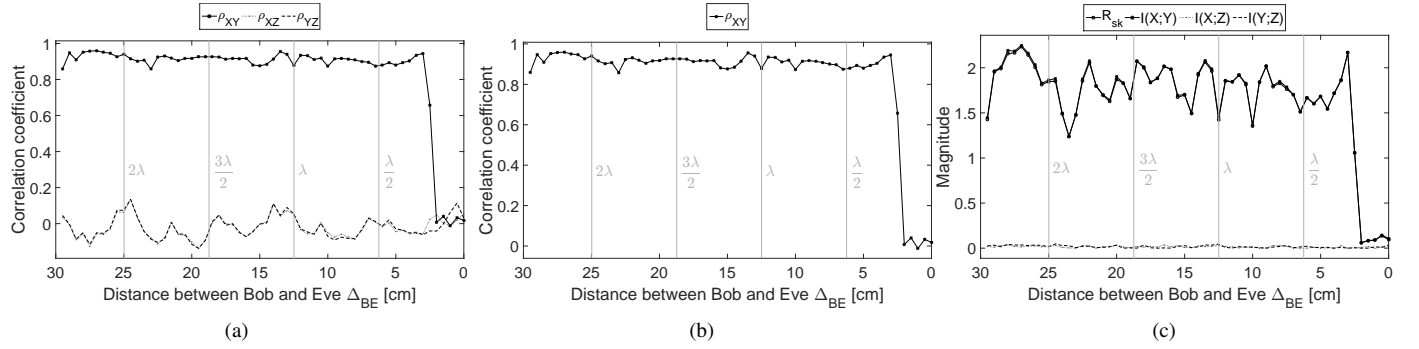


Fig. 77. Evaluation results of v_k^{de} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 22.

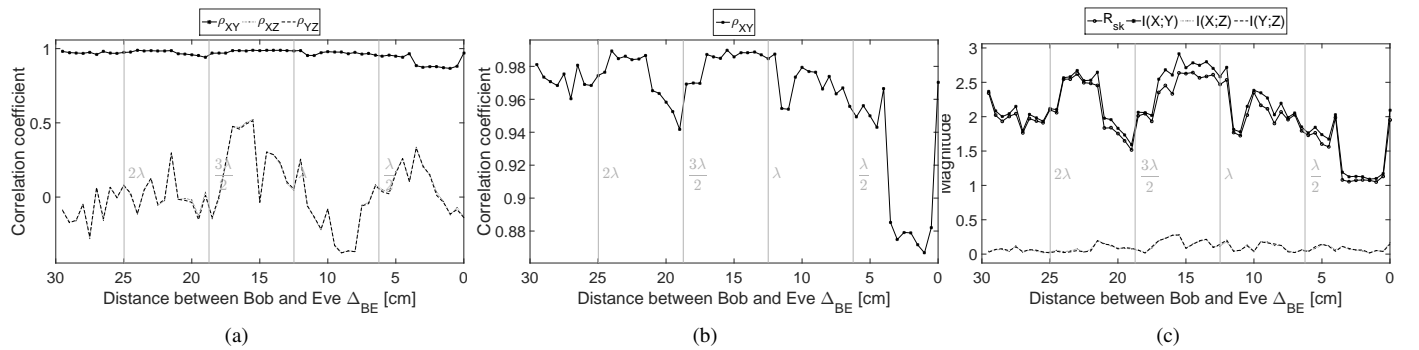


Fig. 78. Evaluation results of v_k . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 23.

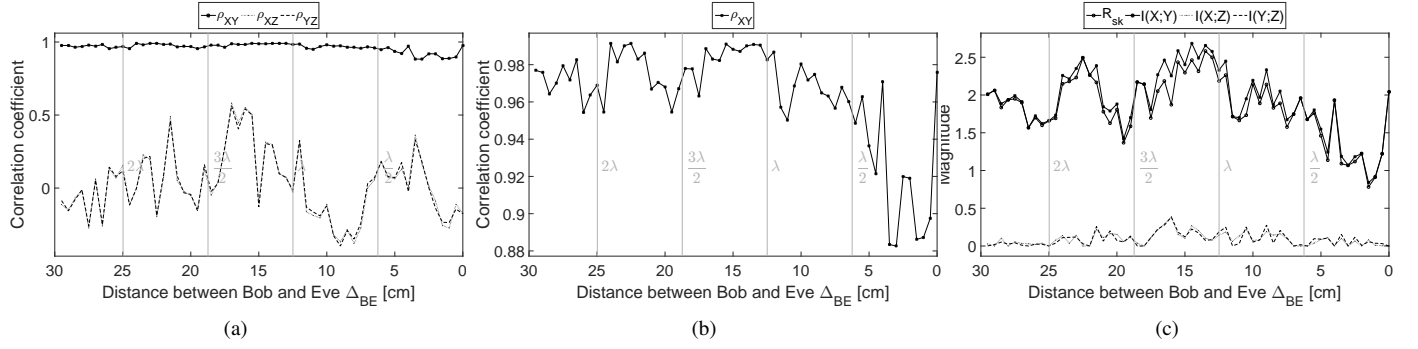


Fig. 79. Evaluation results of v_k^{ds} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 23.

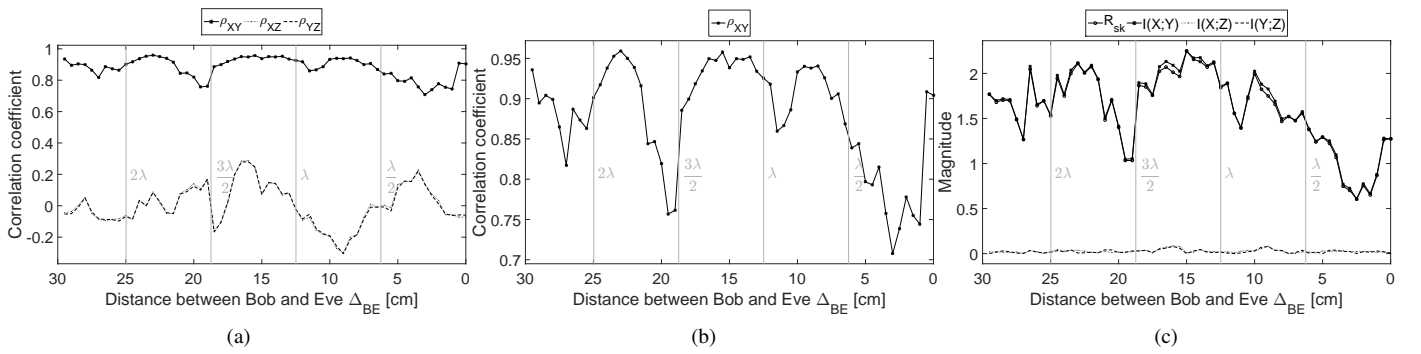


Fig. 80. Evaluation results of v_k^{dc} . In (a) and (b) the cross-correlations is given; in (c) the mutual information as well as R_{sk} is given. Position 23.